2016

GPS Signal Authentication Using INS - A Comparative Study and Analysis

Manickam, Sashidharan

UNIVERSITY OF CALGARY

GPS Signal Authentication Using INS – A Comparative Study and Analysis

by

Sashidharan Manickam

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

GRADUATE PROGRAM IN GEOMATICS ENGINEERING

CALGARY, ALBERTA

SEPTEMBER, 2016

Abstract

Global Navigation Satellite System (GNSS) signal spoofing is an emerging threat to civilian GNSS receivers. Inertial Navigation Systems (INS) are often integrated with GNSS for accurate positioning and navigation, and to bridge GNSS outages in cases where GNSS-only navigation is not feasible. Inertial observations, being self-contained, are not easily spoofed and this redundant information can be used to authenticate GNSS observations.

This thesis presents a comparative study and analysis of the GNSS signal authentication limits using INS in terms of minimum detectable blunder while using different grades of GNSS/INS integrated systems to detect/identify a fault in GPS observation. Results show that for lower spoofing dynamics and longer spoofing duration, all sensor grades fail to detect the GNSS spoofing error immediately. When the spoofing dynamics are high, a high quality INS provides better GNSS signal authentication performance. GNSS/INS integration provides a marginal improvement in the detection/identification performance of spoofed GNSS observations.

Preface

Some part of this thesis contain materials from the peer-reviewed conference paper:

Manickam, S. and K. O'Keefe (2016) "Using Tactical and MEMS Grade INS to Protect Against GNSS Spoofing in Automotive Applications", in *Proceedings of ION GNSS+ 2016*, 12-16 September, Portland, OR, U. S., 11 pages.

Acknowledgements

I would like extend my whole-hearted gratitude to everyone who have supported throughout my stay and my studies in Calgary. There are some people whom I want to thank and mention...

- My parents, KR. Manickam and Lakshmi for providing me all the love, care, support and freedom to do whatever I wish throughout my life and for what I am today. I also thank my aunt Saraswathi, Raja, Selvam and their family including the little kid Abhishek for taking care of my mother in India during my stay in Calgary.
- My supervisor, Dr. Kyle O'Keefe. My graduate studies would not have been possible without his continuous guidance, financial support and encouragement throughout my studies. His moral support and continuous motivation during all the tough times is invaluable. He is one of the kindest person I have ever met, and it has been an excellent learning experience and a privilege to work with him.
- Dr. Vyasaraj Guru Rao, for his advice and motivation to pursue my graduate studies. Five years of my work at Accord Software and Systems Pvt. Ltd, India in various projects under his leadership is indeed the foundation for my professional career as well as the starting point for my graduate studies. I sincerely thank Dr. Jayanta K Ray and the entire Accord's management for giving me the opportunity to work and learn at the same time.
- Shruthi D. Nayak and Niranjana Vagle, for making me feel at home always with their care, support and excellent food. Special thanks to Smt. Malathi D. Nayak for taking care of me like my mother during the last few months in Calgary and a special mention to the little angel Aaradhya.
- Dr. Naveen GS and Dr. Srinivas Bhaskar. Their advice and guidance has helped me to be a better person both personally and professionally. I thank them for their continuous

inspiration and motivation from the beginning of my professional career and my studies here at the U of C.

- Dr. Thyagaraja Marathe, Dr. Vijaykumar Bellad for helping with my research and answering all my doubts and questions with at most patience, and Dr. Ranjeeth Kumar for his help during the initial stages of my travel and my stay in Calgary.
- Rakesh Kumar, Vimal Bhandari, Chandra Tjhai, Paul and Laura Norman for their assistance during the data collection. Srinivas Tantry for helping me throughout my studies with his intellectual prowess and for his time to review my technical writing.
- The entire group of friends in Calgary. Ashwitha, Suvarna, Sujay, Nahal, Ahmad Shafati, Pavana, Kavya, Aruna, Samata, Simmer, Erin Kahr, Dr. Anup Dhital, Dr. Sajan Mushni, Jyothi, Sahasra and Ali Prisiavash for making my days in Calgary a truly memorable one.
- All my friends from India, especially Sumadhva B. Pappu for their wishes, support and motivation to pursue my graduate studies.
- All the Geomatics department staffs and my coursework instructors for helping me complete my graduate studies.
- Dr. Farnaz Sadeghpour and Dr. Yang Gao, for agreeing to be in my examination committee and for their questions, comments and suggestions on my thesis.
- Finally, I acknowledge Prof. Gérard Lachapelle for inspiring and supporting so many students to achieve their academic and professional goals.

To my father, KR. Manickam and my mother, M. Lakshmi

Table of Contents

Abstract ii
Preface iii
Acknowledgements iv
Table of Contents vii
List of Tables ix
List of Figures and Illustrations x
List of Symbols xii
List of Abbreviations xv

CHAPTER ONE: INTRODUCTION 1
1.1 GNSS Spoofing 2
1.2 GNSS Spoofing Detection Literature Review 3
1.2.1 Integrated GNSS Authentication Services 3
1.2.2 Aided GNSS Authentication Services 5
1.2.3 Inertial Sensor Based GNSS Authentication 8
1.3 Objectives 10
1.4 Scope 10
1.5 Proposed Work 11
1.5.1 Methodology 14
1.6 Thesis Outline 15

CHAPTER TWO: ESTIMATION AND FAULT DETECTION OVERVIEW 17
2.1 Global Positioning System 17
2.1.1 L1 C/A signal 18
2.2 Inertial Navigation System 21
2.2.1 Local-level Frame (LLF or ENU-frame) 23
2.2.2 Earth Centred Earth Fixed Frame (ECEF or e-frame) 23
2.2.3 Body Frame (b-frame) 23
2.2.4 INS Mechanization 24
2.3 GPS/INS Integration 26
2.3.1 Loose Coupling 27
2.3.2 Tight Coupling 28
2.4 Estimation Overview 29
2.4.1 Least-Squares (LS) 29
2.4.2 Kalman Filter (KF) 32
2.4.2.1 GPS-only EKF 34
2.4.2.2 GPS/INS Integrated EKF 37
2.5 Hypothesis Testing 40
2.5.1 Fault Detection 41
2.5.2 Fault Identification 41
2.5.3 Model adaptation 42

CHAPTER THREE: STATISTICAL RELIABILITY ANALYSIS 44
3.1 Statistical Reliability Analysis 44
3.1.1 GPS-only LS 45

3.1.2 GPS/INS Integration EKF 47
3.2 Loose and Tight Coupling Comparison 48
3.3 GPS/INS Combinations 48
3.4 Results 50
3.4.1 N-grade GPS with T and MH-grade IMU 51
3.4.2 A-grade GPS with T, MH and ML-grade IMU 54
3.4.3 M-grade GPS with ML-grade IMU 56
3.5 Summary 58

CHAPTER FOUR: EXPERIMENTAL RESULTS 61
4.1 Experimental Setup 61
4.2 Lever-Arm Compensation 64
4.3 Spoofing Simulation and Results 65
4.3.1 Spoofing Profile 1 67
4.3.1.1 Epoch-by-epoch LS 69
4.3.1.2 GPS-Only EKF 70
4.3.1.3 GPS/INS Integrated EKF 70
4.3.1.4 Fault Detection 72
4.3.2 Spoofing Profile 2 74
4.3.3 Spoofing Profile 3 76
4.3.4 Spoofing Profile 4 78
4.4 Review of Smartphone Data Loose Coupling 80
4.5 Summary of Results 82

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS 86
5.1 Conclusions 86
5.2 Recommendations for future work 90

REFERENCES 91

List of Tables

Table 2.1: Power spectral densities for velocity states in GPS-only EKF 37

Table 2.2: Gauss-Markov Parameters for the modelling sensor errors 40

Table 3.1: GPS receiver and IMU specifications 50

Table 3.2: GPS range MDB for satellite PRN 30 59

Table 4.1: Lever-arm offset vectors in body frame 64

List of Figures and Illustrations

Figure 1.1: GPS/INS combinations 13

Figure 1.2: Estimators used for comparison 13

Figure 1.3: Software module block diagram 15

Figure 2.1: Block diagram – Loose coupling 28

Figure 2.2: Block diagram – Tight coupling 28

Figure 3.1: Sky plot during the test duration 46

Figure 3.2: Reference trajectory (Google Earth image) 49

Figure 3.3: MDB values for GPS range observations using N-T combination 52

Figure 3.4: Number of visible satellites 52

Figure 3.5: MDB values for GPS range-rate observations using N, N-T, and N-MH combinations 54

Figure 3.6: MDB values for GPS range observations using A, A-T, A-MH and A-ML combinations 55

Figure 3.7: MDB values for GPS range-rate observations using A, A-T, A-MH and A-ML combinations 56

Figure 3.8: MDB values for GPS range observations using M and A-ML combinations 57

Figure 3.9: MDB values for GPS range-rate observations using M and M-ML combinations 57

Figure 3.10: Comparison of MDB values for different GPS/INS combination 59

Figure 4.1: Faults due for spoofing profile-1 68

Figure 4.2: Fault identification – Spoofing profile1 68

Figure 4.3: Ground Trace with spoofing profile 1 for N and N-T combination. 72

Figure 4.4: Fault detection analysis for varying spoofing errors in satellite PRN 30 73

Figure 4.5: Faults due for spoofing profile 2 75

Figure 4.6: Fault identification – Spoofing profile 2 75

Figure 4.7: Faults due for spoofing profile 3 77

Figure 4.8: Fault identification – Spoofing profile 3 77

Figure 4.9: Faults due for spoofing profile 4 79

Figure 4.10: Fault identification – Spoofing profile 4 79

Figure 4.11: Fault detection for various spoofing error in position for smartphone data in LC mode 82

List of Symbols

Symbol	Definition
b_f	Accelerometer bias (m/s^2)
b_ω	Gyroscope bias (deg/h)
C_r	Variance-covariance matrix of residual vector
C_v	Variance-covariance matrix of innovation vector
c	Speed of light = 299792458 m/s
D^{-1}	Transformation matrix used to transform velocity vector from rectangular coordinates into curvilinear coordinates in ECEF frame.
dt	Satellite clock error (s)
dT	Receiver clock error (s)
d_{iono}	Ionospheric delay (m)
d_{tropo}	Tropospheric delay (m)
$d\dot{\rho}$	Orbital error drift (m/s)
$d\dot{t}$	Satellite clock error drift
$d\dot{T}$	Receiver clock error drift
$\tilde{f}^b$	Specific force vector measured by the accelerometer in body frame (m/s^2)
f^b	True specific force vector (m/s^2)
$f_{Doppler}$	Doppler frequency observation
H	Design matrix
H_0	Null hypothesis
I	Identity matrix
K	Kalman gain matrix
LA^x	Lever arm offset vector at *x* frame of reference
m_x	Multipath error for observation *x*
m	Number of states
N_ω	Non-orthogonality of the gyroscope triad error
N_f	Non-orthogonality of the accelerometer triad error
$N_{1-\alpha/2}$	Standard normal distribution at $1-\alpha/2$
$N_{1-\beta}$	Standard normal distribution at $1-\beta$
n	Number of observations
P	Variance-covariance matrix of state vector
P	Pseudorange measurement (m)
Q	Process noise variance-covariance matrix
q_c	Power spectral density of states
R	Observation variance-covariance matrix
R_a^b	Transformation matrix from co-ordinate frame *a* to co-ordinate frame *b*
r	Residual vector

Symbol	Definition
S_f	Accelerometer scale factor error (m/s^2)
S_ω	Gyroscope scale factor error (m/s^2)
v	Innovation vector
x	State vector
$\hat{\mathrm{x}}$	Estimate of state vector
z	Measurement/observation vector
α	Probability of false alarm
β	Probability of missed detection
$(\beta)_x$	Reciprocal of time constant for quantity *x*
$(\sigma)_x$	Standard deviation of quantity *x*
$\varepsilon(f)$	Accelerometer sensor noise
$\varepsilon(\omega)$	Gyroscope sensor noise
$\varepsilon_{\dot{\Phi}}$	Noise due to Doppler (m/s)
ε_P	C/A code noise (m)
ξ	Test statistic for residual/innovation testing
ρ	Geometric range (m), which is the geometric distance between the satellite and receiver
$d\rho$	Line of Sight (LOS) orbital errors
$\Phi_{k,k-1}$	State transition matrix
Δt	Prediction time interval
∇_{MDB_i}	Minimum Detectable Blunder for i^{th} observation
$\chi^2(\mathrm{n}_k - \mathrm{m}_k)$	Chi-squared distribution with $\mathrm{n}_k - \mathrm{m}_k$ degrees of freedom
$\chi^2_\alpha(\mathrm{n}_k - \mathrm{m}_k)$	Chi-squared distribution with $\mathrm{n}_k - \mathrm{m}_k$ degrees of freedom at α significance level
δ_0	Non-centrality parameter
$\delta\hat{\mathrm{x}}$	Estimate of state error vector
δb_r	GPS receiver clock offset (m)
δd_r	GPS receiver clock drift (m/s)
δr^l	Position state error vector in local geodetic frame consisting of Latitude (radians), Longitude(radians), and Height (m) (WGS-84)
$(\delta\varphi, \delta\lambda, \delta h)$	(Latitude error, Longitude error, Height error)
δv^l	Velocity state error vector in ENU frame (m/s)
$\delta\varepsilon^l$	Attitude state error vector consisting of roll, pitch and Azimuth angles (radians)
δb_ω	Gyroscope random bias error (rad/s)
δS_ω	Gyroscope scale factor error (ppm)

Symbol	Definition
δb_f	Accelerometer random bias error (m/s)
δS_f	Accelerometer scale factor error (ppm)
δg^l	Gravity vector computed by a gravity model that can approximately model the Earth's gravity field at the user location
ω_{ie}^l	Angular velocity vector of the Earth's rotation interpreted in LLF
Ω_{ab}^c	Skew-symmetric matrix corresponding to ω_{ab}^c
ω_{el}^l	Angular velocity vector due to change ion orientation of the LLF with respect to Earth interpreted in LLF
$\dot{\Phi}$	Rangerate measurement (m/s)
$\dot{\rho}$	Geometric range-rate (m/s),
$\tilde{\omega}_{ib}^b$	Angular rate vector measured by the gyroscope vector (deg/h)
ω_{ib}^b	True angular rate vector (deg/h)
λ_{L1}	Wavelength of L1 signal
$(\bullet)^-$	Quantity $(\bullet)$ before measurement update
$(\bullet)^+$	Quantity $(\bullet)$ after measurement update
$(\bullet)_k$	Quantity $(\bullet)$ at epoch *k*

List of Abbreviations

Abbreviation	Definition
A	Automotive grade GPS
BPSK	Binary Phase Shift Keying
C/A code	Coarse/Acquisition code
CDMA	Code Division Multiple Access
ECEF	Earth Centred Earth Fixed
EKF	Extended Kalman Filter
ENU	East North Up
GATE	Galileo Test and Development Environment
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
INS	Inertial Navigation System
IMU	Inertial Measurement Unit
KF	Kalman Filter
LLF	Local-Level Frame
LS	Least Squares
M	Smartphone grade GPS
MDB	Minimum Detectable Blunder
MEMS	Microelectromechanical Systems
MH	Automotive MEMS grade IMU
ML	Smartphone MEMS grade IMU
N	Navigation grade GPS
NMA	Navigation Message Authentication
P-code	Precise code
PRN	Pseudo Random Number
RAIM	Receiver Autonomous Integrity Monitoring
RMS	Root Mean Squared
RSS	Received Signal Strength
RTK	Real-Time Kinematic
SBAS	Satellite Based Augmentation System
SSSC	Spread Spectrum Security Code
SV	Satellite Vehicle
T	Tactical grade IMU
TCXO	Temperature Compensated Crystal Oscillator
VSD	Vestigial Signal Defense
VCM	Variance-Covariance Matrix
WGS	World Geodetic System
XO	Crystal Oscillator

Chapter One: INTRODUCTION

Global Navigation Satellite Systems (GNSS) have become an indispensable source of positioning, navigation and timing over the past two decades. Various applications such as cellular networks, smartphones, surveying, freight tracking, power grid synchronization, and time-stamping financial transactions use GNSS. This calls for a more secure and reliable positioning and timing service. All GNSS services provide an open civilian signal and an authorized military signal that is encrypted. Unlike the military signal, GNSS civilian services are not secured and hence are more vulnerable for jamming and spoofing attacks. All the applications mentioned above use GNSS civilian signals and therefore jamming or spoofing these signals could mislead the user with wrong navigation and timing solution.

Jamming refers to broadcast of high power interference signals at the GNSS signal frequency. This may cause adverse effects in signal reception and the receiver loses track of the GNSS satellites. Usually jamming can be detected and there are many methods proposed to mitigate jamming effects (Jafarnia-Jahromi et al. 2013, Borio et al. 2008, Lindström et al. 2007, Seco-Granados et al. 2005, Gromov 2002). GNSS spoofing is a more sophisticated attack intended to fool the GNSS receiver and misguide the user with false positioning and timing data. Spoofing signals that are broadcast are very similar to those of authentic GNSS signals; therefore, it is very difficult for a receiver to detect and mitigate such spoofing attacks. Many research works have proposed methods to detect and mitigate GNSS spoofing attacks, which are reviewed in section 1.2. In order to ensure security and reliability of the GNSS signal during such spoofing attacks, detection and identification of such spoofing errors are necessary. Various methods of GNSS signal spoofing and proposed signal authentication methods are described in section 1.1.

1.1 GNSS Spoofing

GNSS signal spoofing is the transmission of GNSS-like signals in an attempt to steer the tracking loops of a GNSS receiver and manipulate the navigation and timing solutions. There are several documented spoofing techniques with varying levels of sophistication; the simplest method is to use a GNSS signal simulator to transmit or radiate signals at high power. In this case, the spoofer is not time-synchronized with the GNSS satellite signals, however a nearby GNSS receiver may lock on to the spoofing signal and provide an erroneous position and time estimate. This method is known to work as it is exactly how GNSS simulation for testing and research is conducted, albeit with the signal confined to a co-axial cable between the simulator and the device under test. In this case, the spoofer in this case is not synchronized in time as well as data with the actual satellite signal.

An intermediate type of spoofer is one that transmits spoofing signals that are time-synchronized with the satellite and the target receiver. This requires the spoofer to monitor the GNSS signal in space and to estimate the navigation solution of the target receiver (Ledvina et al. 2010). This type of spoofing is relatively difficult to detect or mitigate. A portable GPS civilian spoofer was developed by Humphreys et al. (2008) to provide an asses the spoofing threat.

The most sophisticated attack involves time synchronized spoofing signals broadcast from a network of coordinated intermediate type spoofers that are aligned with the data content, time and the spatial distribution of the visible GNSS satellites. This method of spoofing is very difficult to realize, but has been implemented in the Galileo test and development environment (GATE) project as a test-bed for Galileo receivers (Heinrichs et al. 2008, Wittmann et al. 2000).

1.2 GNSS Spoofing Detection Literature Review

Several anti-spoofing techniques broadly classified as spoofing detection and spoofing mitigation have been proposed in the available literature recently (Jafarnia-Jahromi et al. 2013, Jafarnia-Jahromi et al. 2012, Pozzobon et al. 2010, Correia et al. 2013, Scott 2012, Montgomery 2009, Humphreys et al. 2008, Wen, Huang et al. 2005, Scott 2003). Various research works in GNSS different spoofing detection methods are summarised in Wesson et al. (2012). Spoofing detection is discriminating the spoofing attack, whereas spoofing mitigation is neutralizing the effect. Primarily, in order to detect the spoofing attack, methods to authenticate the GNSS signals are required, especially for the civilian GNSS signals that are under severe threat as the signal structure is openly available to all users. There are two broadly classified approaches for GNSS signal authentication as described below (Pozzobon et al. 2010).

- Integrated GNSS authentication services
- Aided GNSS authentication services

1.2.1 Integrated GNSS Authentication Services

The methods under this classification involve integrating an authentication mechanism as a part of the signal for the civilian GNSS signals. All the methods described here are proposed to be implemented in the signal structure domain broadcasted from the satellite that shall be used by the GNSS receiver to authenticate valid GNSS signals.

- **Cryptographic Methods:** The strategies behind these methods rely on using an additional unpredictable security code along with the pseudo-random codes that modulate the GNSS carrier signals. This security code is predicted on-the-fly and used for authentication. Though this method is not fool-proof, it gives an additional probabilistic security from spoofing. GNSS signal authentication using cryptographic methods have been proposed by

Kuhn (2004), Kuhn (2010), Pozzobon et al. (2010), Wesson et al. (2012) and Humphreys (2013).

- **Spread Spectrum Security Code (SSSC):** This method was proposed to be implemented in GPS L1C, a new GPS signal that is designed for civilian use (Department of Defense 2013). The GPS L1C consists of a data channel and a pilot channel. Unpredictable SSSCs are interleaved with the GPS L1C spreading code on the L1C data channel and code tracking occurs on the pilot channel. Once L1C signal is tracked, receiver can predict when the next SSSC will be broadcast but not its exact sequence. Upon reception of an SSSC, the receiver stores the front-end samples corresponding to the SSSC interval in memory. A cryptographic digital key used to generate the SSSC is later transmitted over the navigation message. The receiver keeps storing the SSSC codes received, and after receiving the digital key, the receiver generates a copy of the actual transmitted SSSC and correlates the generated SSSCs with the stored SSSCs. If the correlation falls below a pre-determined threshold, spoofing is detected. Using a high chipping rate for SSSCs makes it difficult for the spoofer to estimate and replay it in real-time. This offers a strong spoofing defense (Wesson et al. 2012, Scott 2012, Scott 2003). In order to spoof the SSSCs the spoofer requires a high-gain antenna and also very directive, multiple high-gain antennas or a multichannel digital beam-former is needed to successfully receive SSSC chips directly for all satellites in view.
- **Navigation Message Authentication (NMA):** GPS L2C and GPS L5 are the additional GPS signals that are designed specifically to meet the commercial application requirements. Both L2C and L5 Navigation data structure have broadcast message type architecture similar to Satellite-Based Augmentation System (SBAS) messages

(Department of Defense 2013). This method authenticates GNSS signal using an additional authentication message, which is sent every 5 minutes as a part of the broadcast message types along with a public digital key signature algorithm. A digital key is an encrypted data set that is embedded with the satellite broadcast navigation data. Two distinct digital keys, one public and one private are proposed to be used. The private key is known only to the control segment and space segment. This private key will be used to sign the other message types and it is used to authenticate the signature in the authorization message. Though the corresponding public key would be freely available to everyone, it is difficult for an off-the-shelf generator to generate and transmit simultaneously in real-time. It is still possible, however the spoofer would be required to read the data stream in near real-time and replay it instantaneously (Wesson et al. 2012, Wesson et al. 2011, Scott 2003). A comprehensive review of the proposed NMA methods and the design used for GNSS systems is provided in Caparra et al. (2016).

- The NMA and SSSC methods can be combined to have a highly effective authentication technique. The drawback in this scheme is the authentication delay as the authentication cannot occur until the authentication message is received. The SSSC method also has memory requirements for the receiver in order to store the received SSSC (Scott 2003).

1.2.2 Aided GNSS Authentication Services

All the methods described in section 1.2.1 require changes in the broadcast signal structure and hence can only be used in the future GNSS signals. To authenticate the existing GNSS signals, techniques must be developed and applied to the user segment. Such techniques are classified as aided GNSS authentication services. The basic idea for the methods under this classification is to make use of the existing GNSS civilian signals such as GPS L1 C/A by employing techniques at

the GNSS receiver's antenna and/or the signal processing algorithms. There are various techniques to detect the spoofing attack such as:

- Received Signal Strength (RSS) monitoring: This method makes use of the difference in the received signal power signals between the spoofed and authentic GNSS signals (Scott 2012). A simple spoofer using a GNSS simulator can be easily detected using RSS monitoring, and detailed experimental analysis of this method is provided in Jafarnia-Jahromi et al. (2012).
- Spatial coherency analysis: This method relies on the assumption that the spoofing signals of all the satellites are transmitted from a single source. The detection of the spoofing attack is done exploiting the spatial coherency of the received signals. Using appropriate antenna-array processing techniques, spoofing signals can also be mitigated by steering a null towards the direction of the spoofer (P. Montgomery 2009, Jafarnia-Jahromi et al. 2013).
- P(Y) code dual-receiver correlation: In this technique, one reference receiver is stationed in a secure location to track and authenticate L1 C/A signals with receiver-encrypted P(Y) codes. The secure receiver uses the known timing and phase relationships between the C/A code and P(Y) code to isolate the P(Y) code. The secure receiver then sends raw samples (codeless), encrypted with standard W-codes (semi-codeless) (Wesson et al. 2012) over a secure network to the other GNSS civilian receivers. The user GNSS receivers then correlate the locally extracted P(Y) samples with the W-code estimates from the secure receiver. Under spoofing attack, this correlation power drops below a statistical threshold thereby enabling the receiver to detect spoofing. The disadvantage of this method is that it uses P(Y) code and the link between the secure receiver and the other GNSS receiver has to be reliable (Wesson et al. 2012, Psiaki et al. 2013).

- Another strong spoofing defense is the angle-of-arrival defense mentioned in the Volpe report, which is reviewed empirically in Montgomery et al. (2009). This method uses multiple antenna arrays and signal processing methods to detect the angle of arrival of the spoofed signal and use beamforming techniques to mitigate spoofing. This method is only effective if the spoofing signal is coming from a different direction than the real signal and thus can be used to mitigate both simple and intermediate spoofing attacks but cannot defend against a sophisticated attack (Wesson et al. 2012).
- Cooperative GNSS authentication is proposed by Heng et al.(2013). In this method, the signal received by the user receiver is checked against that received by several other cross-check receivers connected in a network. Each check provides a decision on the authenticity of the signal received by the user receiver. An aggregation of these decision leads to the final decision regarding the authenticity of the GNSS position. This method requires a network of interconnected receivers, and so the disadvantage is that reliability of each ad-hoc cross check receiver is less. Therefore, using a less reliable cross check receiver would cause false alarms and reduce the authentication performance.
- Vestigial Signal Defense (VSD): An extensive study and performance evaluation of this method is provided in Wesson et al. (2011). This method uses a software-based, receiver autonomous anti-spoofing technique. If the spoofer does not generate a phase-aligned nulling signal at the phase center of the target GNSS receiver, a vestige of the authentic GNSS signal remains and creates distortion of the complex correlation function. This distortion is monitored to detect spoofing attack (Wesson et al. 2012).

A detailed review of all these methods is given in Wesson et al. (2012) and Ledvina et al. (2010). All these methods are indeed effective but the downside is that all require computationally

intensive signal processing algorithms and/or additional sophisticated antenna-arrays (Jafarnia-Jahromi 2013, Akos 2012). Considering the fact that inertial sensors are available in most consumer navigation devices, another approach is to use the redundant INS observations that are not affected by a GNSS spoofing attack as a source of information to authenticate GNSS. The method of using INS to authenticate GNSS is discussed in Section 1.2.3.

1.2.3 Inertial Sensor Based GNSS Authentication

Inertial navigation system (INS) are navigation system that works on the principle of dead reckoning from a known initial position, velocity and attitude using measurements from accelerometers (accelerations) and gyroscopes (rotation rates). INS and GNSS are often integrated in various applications, whenever available and possible, to provide an integrated navigation solution. Unlike GNSS where the measurements are made from a satellite signal, INS are self-contained and do not rely on any external measurement sources. So an error in GNSS due to a spoofing attack does not affect the INS navigation solution. Taking advantage of this in a GNSS/INS integrated system, the possibility of using this redundant information to detect a spoofing attack on GNSS. Two types of approaches can be used in GNSS/INS integrated system to authenticate GNSS signals:

- Method 1: A straight-forward approach in using inertial sensor output for GNSS authentication is to compare an INS-derived position solution with the GNSS-derived position solution. This method can be used in a loosely coupled GNSS/INS integration scheme.
- Method 2: Second approach is to use a residual based Receiver Autonomous Integrity Monitoring (RAIM) with inertial navigation sensors a proposed in Khanafseh et al (2014).

This method monitors discrepancies between spoofed GNSS measurements and INS measurements in a GNSS/INS tightly-coupled navigation system.

In both methods, If the spoofer has complete knowledge regarding the user dynamics and the motion trajectory, the spoofer could easily take over the receiver by introducing finer errors such that the navigation estimation filter diverges without detection. This reduces the possibility of detecting the spoofing attack. Unlike other methods reviewed in section 1.2.1 and 1.2.2, the INS-based spoofing detection is done at the measurement level in the estimation phase of the receiver.

Very little research has been done so far in GNSS authentication or spoofing detection using INS. An analysis of GNSS protection limits using INS in a tightly coupled architecture has been published by Tanil and Khanafseh (2015) and Khanafseh et al. (2014). In both of these papers, a residuals-based Receiver Autonomous Integrity Monitoring (RAIM) algorithm is proposed using tightly-coupled integration to detect outlier GNSS observations using navigation-grade and tactical grade inertial measurement units (IMUs). However, both of these papers address aerospace applications and the first paper specifically discusses the interaction of this kind of algorithm with the dynamic response of an aircraft actuated by an auto-pilot. In both cases, the GNSS signal is "authenticated" if it is consistent with the navigation solution provided by GNSS, INS and vehicle dynamics model. The ability to detect spoofing using this approach deteriorates rapidly since INS error estimates will adapt quickly to an erroneous GNSS update and hence it is necessary to detect GNSS errors before this occurs. The major disadvantages in using INS-based spoofing detection can be summarized as follows:

- INS-based spoofing detection requires continuous inertial sensor calibration as the position estimate errors and their covariance will continuously grow without bound.

- INS-based spoofing detection has only been tested with high quality sensors that are large size and expensive (Khanafseh et al. 2014) (Jafarnia-Jahromi et al. 2013).

1.3 Objectives

The objective of this thesis is to provide a comparative study and analysis of the GPS signal authentication performance limits in using different grades of INS for GPS spoofing detection.

This thesis focusses on answering the following questions:

1. For a given grade of GPS/INS combination, what are the GPS signal authentication performance limits that can be achieved in terms of Minimum Detectable Blunder (MDB) with a significance level?
2. Are micro-electro-mechanical system (MEMS) grade sensors useful to provide a reasonable GPS signal authentication limits for automotive applications?
3. Since inertial sensors and GNSS receivers are available but not integrated in many automotive and consumer grade devices, is it worthwhile to tightly couple these in order to protect against GNSS spoofing?

1.4 Scope

Following are the points describing the scope of this thesis:

- The analysis done is limited to loose and tight-coupling approaches (reviewed in section 2.3) for GPS/INS integration as these two methods are most commonly used in low-cost automotive applications. Ultra-tight integration methodology is not considered/reviewed as it is not commonly used in consumer grade devices.
- The entire data collection was done using strap down IMUs and so the results presented are applicable only for such systems.

- The experimental data collection is proposed to be done on a land vehicular scenario, and does not apply for a pedestrian hand-held application.
- This thesis focusses on the capability of detecting/identifying individual faulty GPS observations, external reliability is not in scope of this thesis and hence not presented.

1.5 Proposed Work

The methods reviewed in section 1.2.3 for INS-based GNSS signal authentication are more directed towards the use of navigation and tactical grade Inertial Measurement Units (IMU) and are primarily focused on aerospace applications. However, a comparative study and analysis of the GNSS signal authentication performance for various INS grades, especially with low quality MEMS grade sensors have not been provided. A typical automotive application uses a lower grade sensors and the major drawback in using inertial sensor based authentication methodologies in low-cost devices such as smartphones is the poor long-term stability of the sensor errors. The performance analysis will be done using the real GPS/INS data collected in the field for a typical automotive user, which is not done in the previous works. Experimental tests are not reported in the previous works.

Due to the recent advancements in MEMS technology, most modern smartphones are equipped with inertial sensors such as accelerometer, gyroscope, magnetometer and a barometer in addition to a GNSS receiver. Though the primary use of these sensors in smartphone are not for navigation due to large stochastic sensor error and stability over time, this research investigates whether is it worthwhile to have an integrated GPS/INS system using low-end INS with the available resources and specifications to help identifying fault in GPS during a spoofing attack.

In the methods specified in section 1.2.3, the ability to detect spoofing deteriorates quickly due to large INS sensor error drift. Further, in the tightly coupled method, if the spoofing attack is

not detected instantaneously, it may impact the INS error state estimates due to the tight-coupling mechanism and subsequent detection capability will be degraded. A worst case fault profile is when the fault is injected slowly into the GPS measurements, thereby corrupting INS calibration without being detected. So in the work presented in this thesis, multiple test scenarios are defined based on the receiver dynamics and spoofing trajectory dynamics.

Considering the recent advances in sensor quality (mainly in MEMS grade) and the widespread adoptions of GNSS and INS in mass market applications, including automotive and pedestrian navigation, a detailed analysis of GNSS fault (due to spoofing) detection/identification in using low-end MEMS grade IMUs has never been provided. This thesis focuses on analyzing the GNSS fault detection/identification limits whilst using a low-end MEMS-grade IMUs and comparing it with the performance of high-end tactical grade IMUs. Tactical grade IMUs are high quality, less error IMUs that are typically used in military and aerospace applications. The use of tactical grade data in this thesis is to compare the performance of low-end sensors with the high-end counterparts. The choice and classification of the various GPS receiver and IMUs used in this work were based on the measurement quality. The combinations that were used for analysis are as shown in Figure 1.1 with abbreviations shown in red.

The GPS/INS combinations studied were chosen to be reasonable/usable for an automotive application. For example, a Smartphone GPS/Tactical grade IMU (denoted M-T) combination was not chosen because its not practical to integrate a smartphone grade GPS with a tactical grade IMU due to cost and size constraints. Also, for the applications in hand, it is not required to have a such a combination in place. The specifications of the GPS receivers and IMUs used are shown in Table 3.1 as obtained from the manufactures specifications of each. The highest quality of IMUs available are referred to as “Navigation Grade” and are used mainly aboard ships and aircraft,

particularly in military applications. Since it is not practical to use such expensive systems in civilian applications, the navigation grade IMUs were not chosen for analysis in this work.

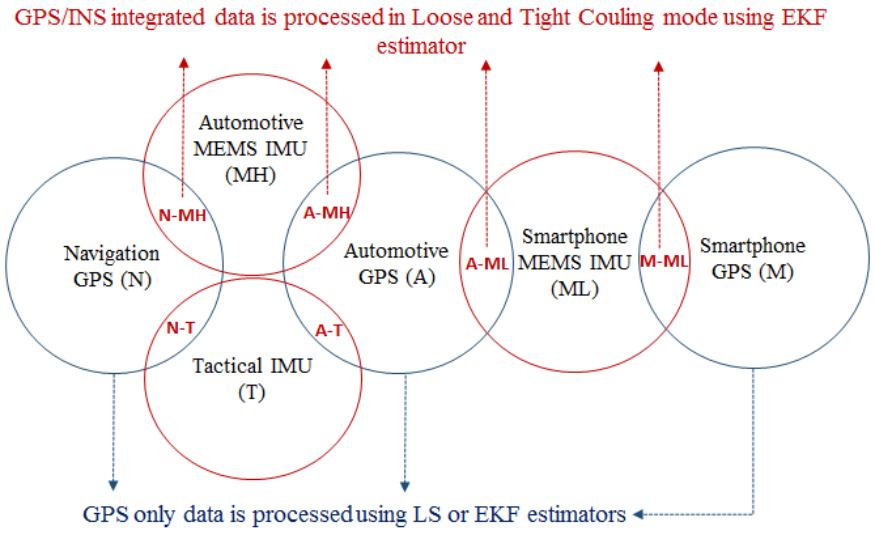

Figure 1.1: GPS/INS combinations

Figure 1.2 shows the block diagram of various estimators implemented in this work for processing GPS-only and GPS/INS integrated observations. A review of these estimation algorithms is presented in section 2.4.

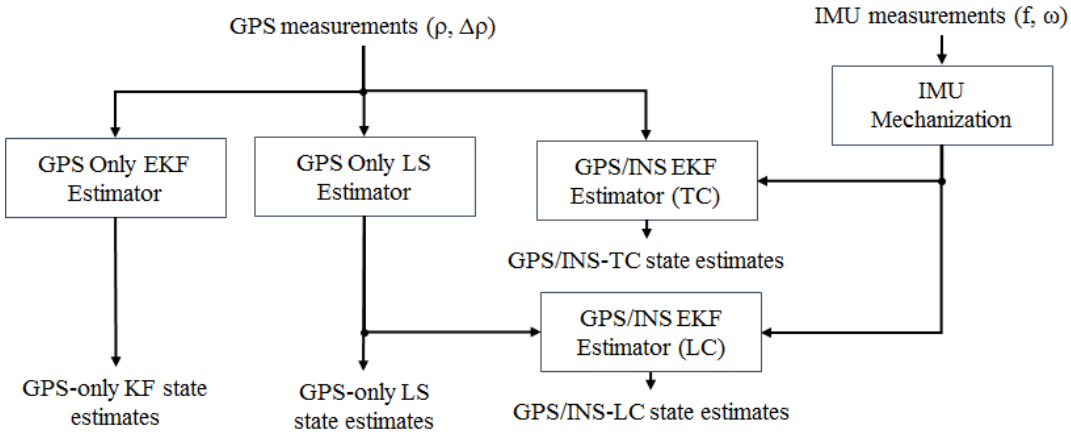

Figure 1.2: Estimators used for comparison

1.5.1 Methodology

The spoofing detection methodology used in this work is based on the innovation/residual testing. The individual GPS observation residuals/innovations are tested against the GPS/INS integrated state estimates to detect the presence of any fault in the GPS observation caused by the spoofing attack. A detailed review of the hypothesis testing is described in section 2.5. It should be noted that fault detection using these methods may be effective against any gross error in a GPS observation (that is errors that exceed the expected levels of uncertainty or noise in each measurement).

In this thesis, the first step is a statistical internal reliability analysis to evaluate the theoretical limits of fault detection/identification capability of the systems under test. The statistical reliability analysis results are then verified by collecting authentic GPS and INS data using the different GPS/INS systems under test and then injecting spoofed GPS observations with different spoofing threat profiles in post-processing.

Figure 1.3 illustrate the block diagram of the software modules used in this work including the spoofing generator module. The spoofing generator module generates the erroneous pseudorange and range-rate observations for the satellite(s) chosen during spoofing configuration. Note that the spoofing error is generated and injected during the post-processing stage and not during the data collection. The detailed description of the various spoofing profiles is given section 4.3.

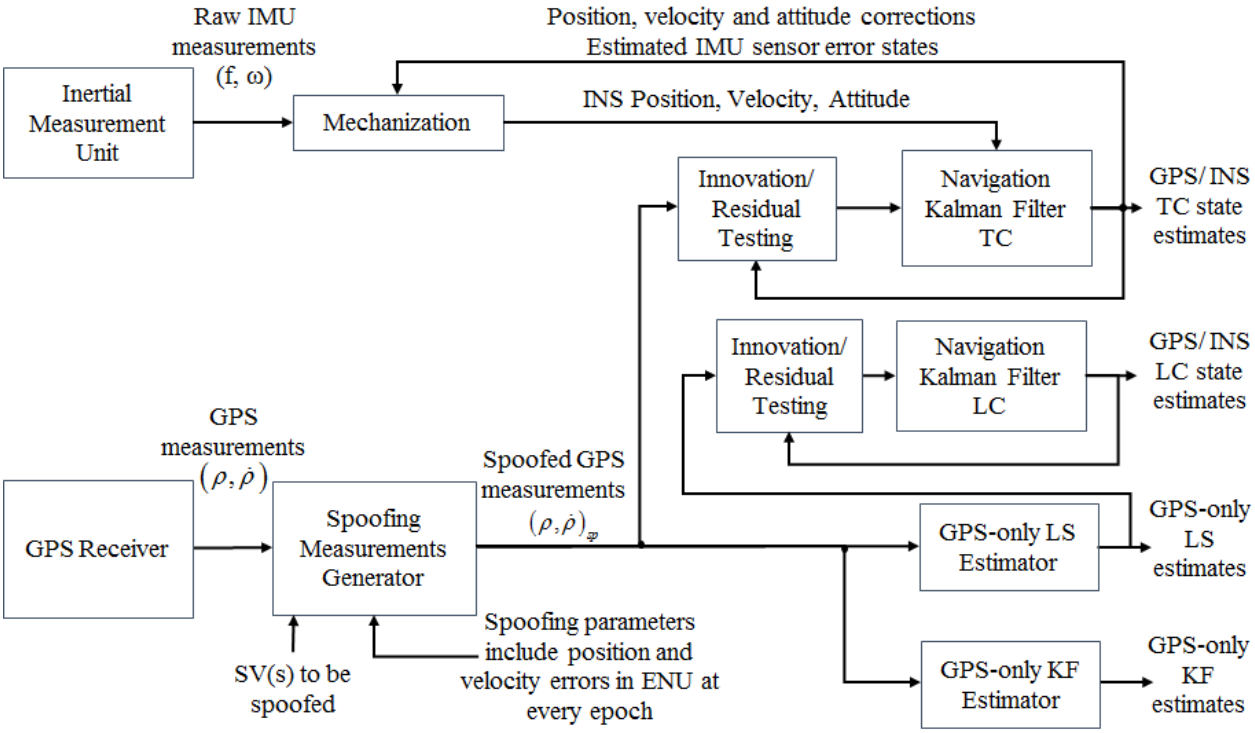

Figure 1.3: Software module block diagram

1.6 Thesis Outline

The thesis is organized as follows:

- Chapter Two reviews the fundamentals of GPS and INS based navigation and the integration methods. An overview of the estimation algorithms used in GPS/INS integrated navigation systems and the corresponding equations are presented followed by the review of fault detection/identification methods used in this work.
- Chapter Three presents the statistical internal reliability analysis using covariance analysis for each of the various grades of IMUs and GNSS receivers. The covariance simulation is useful in evaluating the smallest innovation sequence (blunder) that can be detected. This is the Minimum Detectable Blunder (MDB). The results of the statistical reliability

simulation are shown to provide the theoretical limits of MDB for the GNSS innovation sequences.

- Chapter Four describes the spoofing injection methodology and the various spoofing profiles used followed by the results and analysis of the fault detection/identification performance using the actual GNSS/INS data collected in a sub-urban environment for a vehicular trajectory.
- Chapter Five represents concluding remarks and recommendations for future work.

Chapter Two: ESTIMATION AND FAULT DETECTION OVERVIEW

This chapter provides an overview of the fundamentals of GPS and GPS/INS integrated navigation strategies as precursor for the discussions to follow. First, an overview of the GPS and INS based navigation system is reviewed. Subsequently, an overview of Least-squares (LS) and Extended Kalman filter (EKF) based estimation algorithms and the corresponding equations used in this work are presented. To conclude, the fault detection/identification methodology for a single satellite fault is presented.

2.1 Global Positioning System

The Global Positioning System (GPS) is the satellite-based navigation system developed by the United States Department of Defense under its NAVSTAR satellite program (Parkinson and Spilker 1996). In this thesis, the GPS will be used as an example of a GNSS. The methods described in this thesis could equally be implemented and tested using other GNSS, however GPS is currently the only fully operational GNSS with global coverage. GPS have evolved over decades to provide a wide range of applications. The basic GPS signal structure and receiver architecture is available in various literature (Department of Defense 2013, Parkinson and Spilker 1996, Misra and Enge 2001) and will not be reviewed in detail here. As this thesis focuses mainly on the estimation and positioning module in a GPS receiver, only that relevant material is provided.

The GPS signal consists of the following:

- Navigation data that contains parameters such as satellite orbital, clock, health parameters broadcast to users in real-time at 50 Hz modulation.
- Three types of CDMA based Pseudo-Random Noise (PRN) codes used for ranging measurements namely, Coarse/Acquisition (C/A-code), Precise code (P-code) and the Y-code. C/A code is used primarily as the civilian ranging signal and is also used for

acquisition of P or P(Y) code. The Y-code is used in place of P-code whenever the anti spoofing mode is on, but its available only for the United States and allied military users.

- Both Navigation data and PRN codes are modulated onto three carrier frequencies, namely L1 (1575.42 MHz), L2(1227.60 MHz), and L5 (1176.45 MHz). Only C/A code is modulated on to L1, whereas P-code is modulated on both L1 and L2 carriers. The L5 signal has only been recently added and carriers several open and restricted codes as well as a new navigation message.

There are three basic types of measurements that can be obtained from a GPS receiver to estimate a single-point navigation solution, which are *Pseudorange (code) measurement* (ρ) that are derived from the PRN codes, *Carrier phase measurement* (φ) that is measured using the phase of the incoming carrier, *Doppler measurement* ($\dot{\Phi}$), which is a derivative of the carrier phase measurement caused due to relative motion between the receiver and satellite. However, only the pseudorange and Doppler measurements from L1 C/A signal were only considered in this work as these two measurement types are commonly available from even the lowest cost receivers and hence only the details reagrding those are reviewed in section 2.1.1.

2.1.1 L1 C/A signal

The PRN C/A code modulated on to the L1 carrier is 1 millisecond long at a chipping rate of 1023 Kbps. The code generation method for various satellite PRNs is described in the GPS Interface Control Document (Department of Defense 2013). The navigation data that consists of the satellite ephemerides, system time, satellite clock, and status messages are transmitted at 50 bps and binary phase shift keying (BPSK) modulated with C/A signal. Upon reception of the L1 C/A signal, the GPS receiver makes *Pseudorange (code) measurements* (ρ) measurements from the code phase and *Range-rate measurement* ($\dot{\rho}$) from the Doppler frequency change observed

from the signal. The corresponding observation equations can be written as (Lachapelle & Cannon 2014),

$$P = \rho + d\rho + c(dt - dT) + d_{iono} + d_{tropo} + m_{\rho} + \varepsilon_P \tag{2.1}$$

$$\dot{\Phi} = \dot{\rho} + d\dot{\rho} + c(d\dot{t} - d\dot{T}) - \dot{d}_{iono} + \dot{d}_{tropo} + m_{\dot{\Phi}} + \varepsilon_{\dot{\Phi}} \tag{2.2}$$

where

P	Pseudorange measurement (m)
ρ	Geometric range (m), which is the geometric distance between the satellite and receiver
$d\rho$	Line of Sight (LOS) orbital errors
$dt - dT$	Difference between satellite and receiver clock errors (s)
d_{iono}	Ionospheric delay (m)
d_{tropo}	Tropospheric delay (m)
ε_P	C/A code noise (m)
$\dot{\Phi}$	Rangerate measurement (m/s)
$\dot{\rho}$	Geometric range-rate (m/s),
$d\dot{\rho}$	Orbital error drift (m/s)
$(d\dot{t} - d\dot{T})$	Difference between satellite and receiver clock error drifts (m/s)
m_{ρ}, $m_{\dot{\Phi}}$	Multipath error for pseudorange and range-rate observation respectively
$\varepsilon_{\dot{\Phi}}$	Noise due to Doppler (m/s)
c	Speed of light = 299792458 m/s

The geometric range ρ is the geometric distance between the satellite and the receiver position and can be expressed as,

$$\rho = \sqrt{(x^s - x_R)^2 + (y^s - y_R)^2 + (z^s - z_R)^2} \tag{2.3}$$

where (x^s, y^s, z^s) and (x_R, y_R, z_R) represent the satellite and the estimated receiver position in Earth Centred Earth Fixed Frame (ECEF) co-ordinate frame defined in section 2.2.2. The geometric range-rate $\dot{\rho}$ is the time derivate of the range measured using the Doppler frequency of the signal received from the respective satellite. The relationship between the range-rate and Doppler observation is given by,

$$\dot{\rho} = f_{Doppler} \bullet \lambda_{L1} \tag{2.4}$$

A typical automotive or consumer grade GPS receiver is equipped to receive and decode the Navigation data from the GPS signal and make use of the pseudorange and range-rate observations to estimate the unknown receiver position and velocity using any of the standard estimation algorithms like Least-squares (LS) or Kalman Filtering (KF), which are reviewed in section 2.4. The L1 C/A signal is most widely used in many GPS based navigation applications for civilian users. However, it is easy to spoof this signal (unlike the encrypted military P(Y) code) as the signal structure is publicly available to all users.

Several error sources play a role in the overall accuracy of the GPS navigation solution as shown in Equations (2.1) and (2.2) . A comprehensive review of the orbital, ionosphere, troposphere and multipath errors are provided in Ryan (2002), Skone (1998), Zhang (1999) and Ray(2000) respectively. Differential processing techniques are often implemented to elimiate some of these errors (Petovello 2003). In this work, only single frequency GPS recievers using single-point estimation are considered for testing and analysis because this is the normal mode of operation for existing automotive and smartphone receivers. In single-point mode, these errors can still be reduced. The ionosphere and troposphere errors are compensated using the Klobuchar

model (Klobuchar 1987) for the ionosphere and Hopfield model (Hopfield 1971) for the troposphere, while multipath error is reduced by operating in open sky environments.

This section reviewed the fundamentals of GPS system and the various observations that can be made. Before reviewing with the estimation algorithms used for positioning and naviagtion in GPS (section 2.4), an overview of Inertial navigation system is provided in section 2.2 as a precursor for GPS/INS integrated navigation.

2.2 Inertial Navigation System

Accelerometers and gyroscopes (inertial sensors) measure acceleration and rotation rates of the body on which they are mounted. The fundamental concept of INS is to use these sensor measurements to yield a set of navigation parameters such as position (r^l), velocity (v^l), and attitude (ε^l) in the coordinate frame of choice. This process is referred to as *IMU Mechanization*. For the purpose of this work, mechanization is done in the local-level frame (LLF) (described in section 2.2.1) and is represented by a superscript *l* in the state vector notations. The inertial sensors measurements are always in the body frame *b* (described in section 2.2.3) and in a strap down system, the body frame can be in any direction as the inertial sensors are strapped down to the vehicle. A rotation matrix R_b^l from the body frame to the LLF is established at the beginning using a stationary alignment process. During the initial alignment, the east and north accelerometer measurements are used for levelling the INS (known as accelerometer levelling), and the up gyroscope measurement (known as gyro-compassing) is used to align the INS in heading. For low grade IMUs, gyro-compassing using the gyroscope measurement alone is not feasible as the Earth's rotation cannot be sensed by the gyroscope. This is due to gyroscope errors larger than the Earth's rotation rate. In such cases, an external sensor like a magnetometer or a compass is used to initialise the heading. If GPS is integrated, GPS east and north velocities are used for this

purpose to provide an initial attitude. The expressions for gyro-compassing and accelerometer levelling are detailed in Noureldin et al. (2014). Inertial navigation works well only when the initial position, velocity and attitude of the moving platform is well known prior to the navigation. The measurement models of the accelerometer and gyroscope measurements are given in Equations (2.5) and (2.6) respectively.

$$\tilde{\omega}_{ib}^{b} = \omega_{ib}^{b} + b_{\omega} + S_{\omega}\omega_{ib}^{b} + N_{\omega}\omega_{ib}^{b} + \varepsilon(\omega) \tag{2.5}$$

$$\tilde{f}^{b} = f^{b} + b_{f} + S_{f} f^{b} + N_{f} f^{b} + \delta g + \varepsilon(f) \tag{2.6}$$

where

$\tilde{\omega}_{ib}^{b}$	Angular rate vector measured by the gyroscope vector (deg/h)
ω_{ib}^{b}	True angular rate vector (deg/h)
$\tilde{f}^{b}$	Specific force vector measured by the accelerometer in body frame (m/s^2)
f^{b}	True specific force vector (m/s^2)
b_{f}	Accelerometer bias (m/s^2)
S_{f}	Accelerometer scale factor error (m/s^2)
N_{f}	Non-orthogonality of the accelerometer triad error
b_{ω}	Gyroscope bias (deg/h)
S_{ω}	Gyroscope scale factor error (m/s^2)
N_{ω}	Non-orthogonality of the gyroscope triad error
$\varepsilon(f)$	Accelerometer sensor noise
$\varepsilon(\omega)$	Gyroscope sensor noise

2.2.1 Local-level Frame (LLF or ENU-frame)

The Local-level frame represents a vehicle's attitude and velocity when on or near the surface of the Earth (Noureldin et al. 2014) and the frame used herein is defined as follows:

- Origin: Centre of the sensor frame.
- X-Axis: Pointing towards the east.
- Y-Axis: Pointing towards the true north.
- Z-Axis: Orthogonal to the X and Z axes to complete a right-handed frame by pointing up perpendicular to the reference ellipsoid.

2.2.2 Earth Centred Earth Fixed Frame (ECEF or e-frame)

The Earth-fixed frame used herein is defined as follows (Kaplan and Hegarty 2006):

- Origin: Earth's centre of mass.
- Z-Axis: Parallel to the Earth's mean spin axis.
- X-Axis: Pointing towards the mean meridian of Greenwich.
- Y-Axis: Orthogonal to the X and Z axes to complete a right-handed frame.

2.2.3 Body Frame (b-frame)

The body frame represents the orientation of the IMU axis. In a strap down inertial system used as in this case, the IMU is mounted on the vehicle and assumed to be aligned with the vehicle. The frame used herein is defined as follows (Petovello 2003):

- Origin: Local origin on the body of the vehicle.
- X-Axis: Parallel towards the right of the vehicle.
- Y-Axis: Parallel towards the front of the vehicle.
- Z-Axis: Orthogonal to the X and Z axes to complete a right-handed frame.

2.2.4 INS Mechanization

INS mechanization is the process of converting the above mentioned IMU measurements to the position, velocity and attitude state vectors. IMU mechanization equations can be found in various available literature (Noureldin et al. 2014, Jakeli 2001). The IMU mechanization equation in LLF used in this thesis is shown in Equation (2.7).

$$\begin{bmatrix} \delta\dot{\mathrm{r}}^{l} \\ \delta\dot{\mathrm{v}}^{l} \\ \delta\dot{\varepsilon}^{l} \end{bmatrix} = \begin{bmatrix} D^{-1}\delta\mathrm{v}^{l} \\ R_b^l f^b \varepsilon^l - (2\Omega_{ie}^l + \Omega_{el}^l)\delta\mathrm{v}^l - (2\delta\Omega_{ie}^l + \delta\Omega_{el}^l)\mathrm{v}^l + \delta g^l + R_b^l b_f + R_b^l f^b S_\omega \\ -\Omega_{il}^l \delta\varepsilon^l - \delta\omega_{il}^l + R_b^l b_\omega + R_b^l \omega^b S_f \end{bmatrix} \quad (2.7)$$

where

δr^l Position state error vector in local geodetic frame consisting of Latitude (radians), Longitude(radians), and Height (m) (WGS-84) $(\delta\varphi, \delta\lambda, \delta h)$

δv^l Velocity state error vector in ENU frame (m/s) $(\delta v_e, \delta v_n, \delta v_u)$

$\delta\varepsilon^l$ Attitude state error vector consisting of roll, pitch and Azimuth angles (radians) $(\delta r, \delta p, \delta A)$

$\delta\dot{\mathrm{r}}^l \ \delta\dot{\mathrm{v}}^l \ \delta\dot{\varepsilon}^l$ Time rate of change of potion, velocity and attitude state error vectors in LLF

δb_ω Gyroscope random bias error (rad/s)

δS_ω Gyroscope scale factor error (ppm)

δb_f Accelerometer random bias error (m/s)

δS_f Accelerometer scale factor error (ppm)

R_b^l Transformation matrix from body frame to local-level frame

δg^l Gravity vector computed by a gravity model that can approximately model the Earth's gravity field at the user location

Ω_{ie}^{l} Skew-symmetric matrix corresponding to ω_{ie}^{l} representing the angular velocity vector of the Earth's rotation interpreted in LLF and is expressed in Equation (2.9)

Ω_{el}^{l} Skew-symmetric matrix corresponding to ω_{el}^{l} representing the angular velocity vector due to change ion orientation of the LLF with respect to Earth interpreted in LLF and is expressed in Equation (2.10)

Ω_{il}^{l} Skew-symmetric matrix of the angular velocity vector ω_{il}^{l} that comprises the Earth's rotation rate in inertial-frame expressed in b-frame (Ω_{ie}^{b}) and the change in orientation of the LLF with respect to the ECEF frame as expressed in body frame and is expressed in Equation (2.11).

D^{-1} Transformation matrix used to transform velocity vector from rectangular coordinates into curvilinear coordinates in ECEF frame and is expressed in Equation (2.8)

$$D^{-1} = \begin{pmatrix} 0 & \dfrac{1}{R_M + h} & 0 \\ \dfrac{1}{(R_N + h)\cos\varphi} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2.8}$$

$$\Omega_{ie}^{l} = \begin{pmatrix} 0 & -\omega_e \sin\varphi & \omega_e \cos\varphi \\ \omega_e \sin\varphi & 0 & 0 \\ -\omega_e \cos\varphi & 0 & 0 \end{pmatrix} \tag{2.9}$$

$$\Omega_{el}^{l} = \begin{pmatrix} 0 & \frac{-v_e \tan\varphi}{R_N + h} & \frac{v_e}{R_N + h} \\ \frac{v_e \tan\varphi}{R_N + h} & 0 & \frac{v_n}{R_M + h} \\ \frac{-v_e}{R_N + h} & \frac{-v_n}{R_M + h} & 0 \end{pmatrix} \tag{2.10}$$

$$\Omega_{il}^{l} = R_b^l(\Omega_{ie}^{b} + \Omega_{el}^{b}) \tag{2.11}$$

The INS initial position error may start with a small value, but it tends to increase with time due to the effect of drifting sensor errors. Note that the accelerometer errors are integrated twice to obtain the position and hence an accelerometer sensor error causes a second order (in time) impact on the position solution. Higher grades of sensor (tactical and navigation) have errors that drift more slowly, whereas for lower MEMS grade sensors it is impossible to navigate using INS without external aids. With GPS being available, GPS/INS integration could help in utilising a low-accuracy INS with continuous aiding to keep check of the fast changing sensor errors.

2.3 GPS/INS Integration

A GPS receiver can be considered as a position and velocity sensor using the observations from a constellation of GPS satellites. The errors in the navigation solution depend upon the availability and geometric distribution of the GPS satellites, and other systematic error sources such as satellite clock errors, orbital error, ionospheric and tropospheric errors, multipath etc.

INS provides position, velocity and attitude estimates using inertial sensors such as accelerometers and gyroscopes. The position errors here depend on the quality of inertial sensors and the Earth models. Inertial sensors are prone to various errors as shown in Equations (2.5) and (2.6). INS provides a very good short-term accuracy but the errors are not bounded during the course of a long run. These errors become more complex and vary quickly as the sensor quality

decreases. It is essential to estimate these sensor errors accurately as the sensor errors drift very quickly in a small time duration and these errors limit the overall accuracy of the estimated navigation parameters over time, Integrated GPS/INS system provides more robust, and more reliable navigation service than the stand-alone systems. There are three basic GPS/INS integration strategies, namely;

1. Loose coupling
2. Tight coupling
3. Ultra-tight coupling

The design of a GPS/INS integrated system includes a trade-off between performance and cost and is primarily decided by the application requirements. Ultra-tight coupling, which is an extended version of tightly-coupled system is not in scope of this research and hence will not be reviewed in this thesis.

2.3.1 Loose Coupling

The simplest form of loose coupling uses two separate estimators. The first estimator uses the GPS observations to obtain GPS-derived position and velocity, which are the standard outputs of the GPS receiver. The GPS-derived position and velocity estimates are then coupled with the INS-derived position and velocity estimates in a separate navigation Kalman filter as shown in Figure 2.1. For the purpose of this work, the GPS-only observations processed using an epoch-by-epoch LS estimator were considered as the GPS receiver outputs for loose coupling. This is done primarily to avoid the GPS observations being filtered twice.

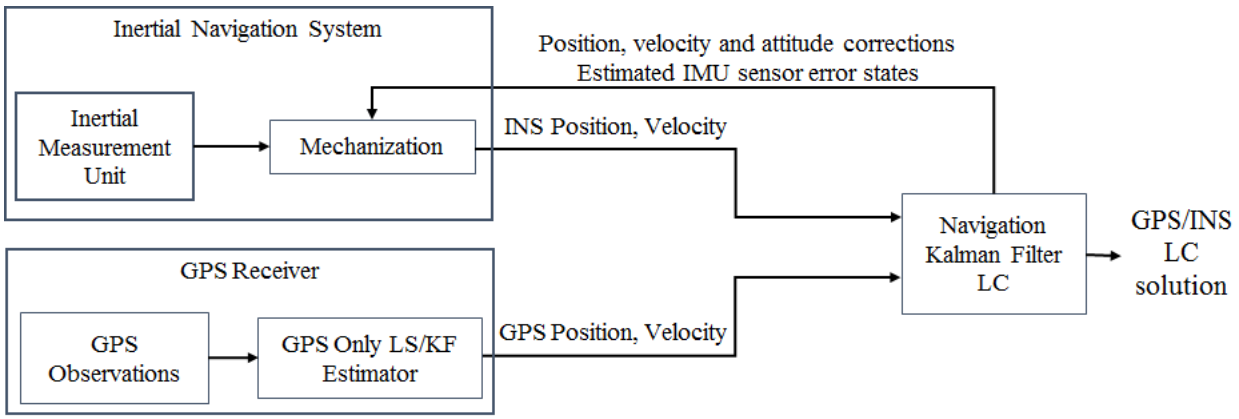

Figure 2.1: Block diagram – Loose coupling

2.3.2 Tight Coupling

In tightly-coupled architecture, there exists only one common navigation Kalman filter that processes the GPS-derived and INS-derived observations as shown in Figure 2.2.

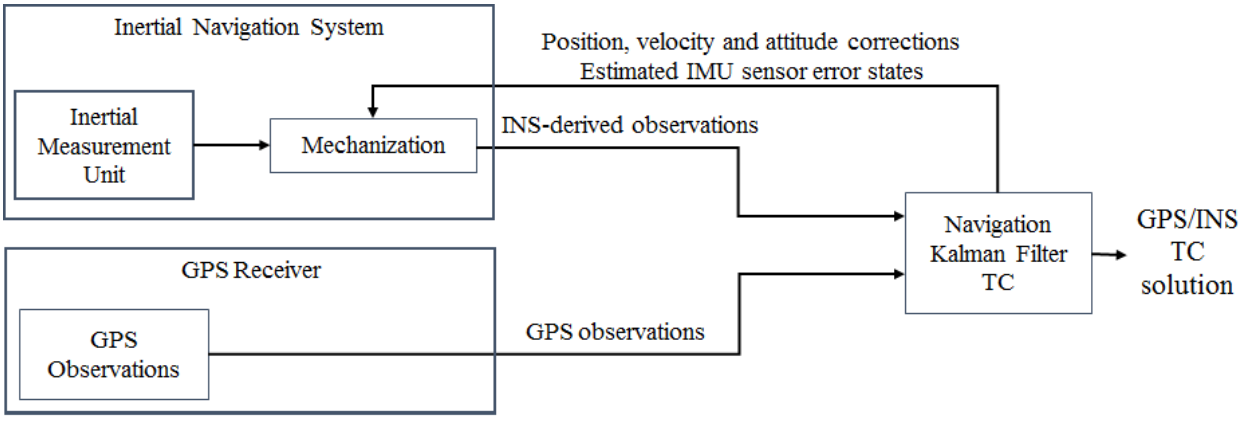

Figure 2.2: Block diagram – Tight coupling

The GPS pseudorange and range-rate observations, which are not the standard GPS receiver outputs for most low-cost GPS receivers, are directly integrated with the INS-derived observations in the KF. Therefore, tight-coupling generally requires software changes in a basic stand-alone GPS receiver to output these observations. The system model in the navigation Kalman filter generally includes the GPS receiver clock offset and drift, and sensor errors such as accelerometer and gyroscope bias and scale factor. Both loose and tight-coupling allow real-time calibration of

inertial sensor errors to improve free inertial performance during GPS signal outages especially in case of low quality INS.

2.4 Estimation Overview

This section provides an overview of different estimation techniques used in this work. Satellite based navigation systems use a set of observations to estimate a desired set of unknown parameters (henceforth referred to as state estimates). The estimation algorithm used for processing GPS-only observations is typically an epoch-by-epoch Least-Squares (LS) approach. In the case of dynamic systems, Kalman filter based estimation is also widely used in various applications. For the purpose of this work, an Extended Kalman Filter (EKF) estimator is used to process GPS-only observations as well GPS/INS integrated observations (in case of loose and tight coupling approaches). GPS-only observations are also processed using an epoch-by-epoch LS algorithm as well and the results are analysed and compared. This section provides an overview of the LS and EKF estimation algorithms used in this work as shown in Figure 1.2.

2.4.1 Least-Squares (LS)

The least squares approach obtains an estimate $\hat{\mathrm{x}}_k$ of the state vector x_k using a set of observations z_k that satisfies an optimality criterion (Kay 1993). In this case, the optimality criterion is defined as the minimization of the weighted sum of squares of residuals. One advantage of using a LS estimator is that there are no probabilistic assumption made on x_k. LS estimation is a most common algorithm used for position and velocity estimation using GPS pseudorange and Doppler observations (Petovello 2013). The basic observation model used for the non-linear LS estimation is,

$$\delta \mathrm{z}_k \approx \mathrm{H}_k \cdot \delta \mathrm{x}_k + \mathrm{v}_k \tag{2.12}$$

$$\delta \mathrm{z}_k = \mathrm{z}_k - \mathrm{h}_\mathrm{k}\left(\hat{\mathrm{x}}_k\right) \tag{2.13}$$

$$\mathrm{H}_k = \left.\frac{\partial \mathrm{h}_\mathrm{k}}{\partial \mathrm{x}}\right|_{x=\hat{\mathrm{x}}_k} \tag{2.14}$$

where $\delta \mathrm{x}_k$ is the state error vector, z_k is the vector of observations vector, $\hat{\mathrm{x}}_k$ is the state vector estimate, consisting of position, velocity, clock offset and clock drift after using the observations z_k, v_k is the measurement noise, h_k is the non-linear vector function that relates the state vector and the observations, H_k is the design matrix, $\delta \mathrm{z}_k$ is the observation misclosure vector at epoch *k*. Note that the GPS observation equations expressed in Equations (2.1) and (2.2) are non-linear. It is necessary to linearize the measurements of this form to use it in the linear estimation algorithms such as LS and Kalman filtering. To linearize, the partial derivatives about an approximate receiver location (x_0, y_0, z_0) are evaluated. The resulting pseudorange observation equation for i[th] satellite after compensating for the ionospheric delay, tropospheric delay and satellite orbital and clock errors is given by,

$$\delta\rho_i = \rho_i - \hat{\rho}_i(\mathrm{x}_0) = \begin{pmatrix} \frac{\partial \rho_i}{\partial x} & \frac{\partial \rho_i}{\partial y} & \frac{\partial \rho_i}{\partial z} \end{pmatrix} \delta \mathrm{x}_k + c(dt - dT) + \mathrm{v}_k \tag{2.15}$$

$$\begin{aligned} \frac{\partial \rho_i}{\partial x} &= \frac{(x_i^s - x_0)}{\sqrt{(x_i^s - x_0)^2 + (y_i^s - y_0)^2 + (z_i^s - z_0)^2}} \\ \frac{\partial \rho_i}{\partial y} &= \frac{(y_i^s - y_0)}{\sqrt{(x_i^s - x_0)^2 + (y_i^s - y_0)^2 + (z_i^s - z_0)^2}} \\ \frac{\partial \rho_i}{\partial z} &= \frac{(z_i^s - z_0)}{\sqrt{(x_i^s - x_0)^2 + (y_i^s - y_0)^2 + (z_i^s - z_0)^2}} \end{aligned} \tag{2.16}$$

where

x_0 Nominal point of linearization based on (x_0, y_0, z_0) and predicted receiver time

$\hat{\rho}_i(\mathrm{x}_0)$ Predicted pseudorange based on x_0

The corresponding range-rate observation equation for i[th] satellite is similarly evaluated with respect to the receiver velocity vector (Misra and Enge 2001). The weighted LS provides the best unbiased estimate if the variance-covariance matrix (VCM) of the GPS observations, R_k, is non-singular with the assumption that the VCM of the estimated state vector P_k is as shown in Equation (2.19). This means there must be at least as many uncorrelated observations available at every epoch as unknown states. The state error vector $\delta\mathrm{x}_k$ is estimated iteratively using,

$$\delta\hat{\mathrm{x}}_k = \left(\mathrm{H}_k^T\mathrm{R}_k^{-1}\mathrm{H}_k\right)^{-1}\mathrm{H}_k^T\mathrm{R}_k^{-1}\delta\mathrm{z}_k \tag{2.17}$$

The full state vector x_k is then obtained by,

$$\mathrm{x}_k = \mathrm{x}_0 + \delta\hat{\mathrm{x}}_k \tag{2.18}$$

$$\mathrm{P}_k = \left(\mathrm{H}_k^T\mathrm{R}_k^{-1}\mathrm{H}_k\right)^{-1} \tag{2.19}$$

The iteration process is continued until the state vector error converges below a sufficiently small threshold relative to the expected accuracy. The design matrix H_k with *n* number of observations for the GPS-only LS estimator used in this work takes the form as shown in Equation (2.20),

$$\mathrm{H}_{k,GPSLS} = \begin{pmatrix} \frac{\partial\rho_1}{\partial x} & \frac{\partial\rho_1}{\partial y} & \frac{\partial\rho_i}{\partial z} & 0 & 0 & 0 & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{\partial\rho_n}{\partial x} & \frac{\partial\rho_n}{\partial y} & \frac{\partial\rho_n}{\partial z} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{\partial\rho_1}{\partial x} & \frac{\partial\rho_1}{\partial y} & \frac{\partial\rho_1}{\partial z} & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \frac{\partial\rho_n}{\partial x} & \frac{\partial\rho_n}{\partial y} & \frac{\partial\rho_n}{\partial z} & 0 & 1 \end{pmatrix} \tag{2.20}$$

The residual vector r_k is the difference between the actual observations and the predicted observations. The residual vector r_k and its covariance C_{r_k} are expressed in Equation (2.21) and (2.22) respectively.

$$r_k = z_k - h_k\left(\hat{x}_k\right) \tag{2.21}$$

$$C_{r_k} = R_k - H_k P_k H_k^T \tag{2.22}$$

2.4.2 Kalman Filter (KF)

The LS equations expressed in section 2.4.1, provide an epoch-by-epoch single point state estimation using either GPS observations only or GPS/INS integrated observations that relate to the state vector. The state estimates are implicitly assumed to be time invariant, without any considerations to the previous or the future values of the states. However, a better estimate can be obtained by considering the time evolution of the state estimates. The Kalman filter (Kalman 1960) algorithm includes the time evolution of the state vector as an additional information, thus paving a way to predict the state vector at a future time instance assuming a system dynamics model.

In case of KF, the non-linear observation models remain the same as the LS case shown in Equation (2.12). The linearized dynamic discrete time system model equation used herein takes the following form (Petovello 2003)

$$\delta x_k \approx \Phi_{k,k-1} \cdot \delta x_{k-1} + w_k \tag{2.23}$$

where δx_k is the state error vector estimate at epoch *k*, $\Phi_{k,k-1}$ is the state transition matrix from epoch *k*-1 to *k*, and w_k is the process noise representing the uncertainties in the system model. Following are the assumptions made in the Kalman filter implementation (Wieser et al. 2004):

1. The process noise w_k and the measurement noise v_k are assumed to be white and uncorrelated with the state vector. Q_k is a positive definite process noise VCM and R_k is the systematic positive definite measurement VCM.

2. The process noise and measurement noise are mutually uncorrelated.
3. An unbiased estimate of the state vector and its covariance matrix is available at the first epoch $k = 0$.

The Kalman filter is a recursive algorithm that computes optimal state estimates with minimum variance by series of prediction and observation update steps as shown below:

State prediction:

$$\delta\hat{\mathrm{x}}_k^{(-)} = \Phi_{k,k-1} \cdot \delta\hat{\mathrm{x}}_{k-1}^{(+)} \tag{2.24}$$

Covariance propagation:

$$\mathrm{P}_k^{(-)} = \Phi_{k,k-1} \cdot \mathrm{P}_k^{(-)} \cdot \Phi_{k,k-1}^T + \mathrm{Q}_{k-1} \tag{2.25}$$

Kalman gain:

$$\mathrm{K}_k = \mathrm{P}_k^{(-)}\mathrm{H}_k^T \left(\mathrm{R}_k + \mathrm{H}_k \mathrm{P}_k^{(-)} \mathrm{H}_k^T\right)^{-1} \tag{2.26}$$

State update:

$$\delta\hat{\mathrm{x}}_k^{(+)} = \delta\hat{\mathrm{x}}_k^{(-)} + \mathrm{K}_k \cdot \delta\mathrm{z}_k \tag{2.27}$$

Covariance update:

$$\mathrm{P}_k^{(+)} = \left(\mathrm{I} - \mathrm{K}_k \mathrm{H}_k\right) \cdot \mathrm{P}_k^{(-)} \tag{2.28}$$

The perturbations due to the linearization of the system model are overcome by using the Extended Kalman Filter (EKF), as the estimated state errors are applied to the original states at every epoch thus resetting state error vector to a null vector (Petovello 2013). This means that the state error prediction step in Equation (2.24) and (2.28) simplifies to,

$$\delta\hat{\mathrm{x}}_k^{(+)} = \mathrm{K}_k \cdot \delta\mathrm{z}_k \quad \because \delta\hat{\mathrm{x}}_k^{(-)} = 0 \tag{2.29}$$

Note that the full state vector prediction step is still used to find the new point of expansion, and the covariance propagation is performed at every epoch. Unlike the LS case, here the statistical reliability analysis is performed on the innovation sequence, which is a function of the predicted

or the best known state estimate prior to the measurement update. The innovation sequence and its VCM has a form similar to that of the residuals in LS case, and are shown in Equations (2.30) and (2.31) respectively.

$$v_k = \mathrm{z}_k - h_k(\hat{\mathrm{x}}_k^{(-)}) \tag{2.30}$$

$$\mathrm{C}_{v_k} = \mathrm{R}_k + \mathrm{H}_k \mathrm{P}_k^{(-)} \mathrm{H}_k^T \tag{2.31}$$

In case of GPS/INS coupling, $\hat{\mathrm{x}}_k^{(-)}$ is the IMU mechanization output at epoch *k*. This is the primary difference in the innovation testing done between LS and EKF estimators. In EKF, innovation testing is done prior to the observation update, whereas in case of LS the residual testing is done after the observation update at any given time epoch *k*. The innovation sequence represents the amount of new information being introduced into the system from the new set of observations at the current epoch. The Kalman gain K_k is a weighting factor that determines how much of this new information should be accepted. The advantage of performing innovation testing prior to update is that the decision whether to use a particular observation or not can be made prior to that observation corrupting the filter solution. Another consideration made is that the state dynamics model is assumed to be time invariant during the prediction time interval.

2.4.2.1 GPS-only EKF

The GPS-only EKF is used to estimate the state observables using the GPS measurements. A 8-state EKF is implemented in MATLAB™ to process GPS-only observations. The state vector x_k include position, velocity, GPS receiver clock offset and clock drift. A constant velocity dynamics model is used in kinematic processing as the chosen vehicular trajectory is a simple motion trajectory in a land vehicle across a sub-urban environment.

The state error vector $\delta \mathrm{x}_k$ and the state transition matrix $\Phi_{k,k-1}$ of GPS-only filter used in this research is represented as,

$$\delta \mathrm{x}_{k,GPSLS} = \begin{pmatrix} \delta r^l & \delta v^l & \delta b_r & \delta d_r \end{pmatrix} \tag{2.32}$$

$$\Phi_{k,k-1} = \begin{pmatrix} I_{3x3} & D^{-1} \cdot \Delta t & 0 & 0 \\ 0 & I_{3x3} & 0 & 0 \\ 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.33}$$

where

δr^l Position state error vector in local geodetic frame consisting of Latitude (radians), Longitude(radians), and Height (m) (WGS-84) $(\delta\varphi, \delta\lambda, \delta h)$

δv^l Velocity state error vector in ENU frame (m/s) $(\delta v_e, \delta v_n, \delta v_u)$

δb_r GPS receiver clock offset (m)

δd_r GPS receiver clock drift (m/s)

Δt Prediction time interval (considered as 1 s)

The design matrix H_k for the GPS-only EKF is given by Equation (2.34) under the consideration that there is *n* number of GPS pseudorange (in m) and range-rate (in m/s) observations each.

$$\mathrm{H}_{k,GPSKF} = \begin{pmatrix} H_{n\times 3} \cdot M_{3\times 3} & 0_{n\times 3} & 1_{n\times 1} & 0_{n\times 1} \\ 0_{n\times 3} & H_{n\times 3} \cdot R_l^e & 0_{n\times 1} & 1_{n\times 1} \end{pmatrix}_{n\times 8} \tag{2.34}$$

The transformation matrices $M_{3\times 3}$ is used to transform the position errors in local geodetic frame to ECEF frame (as the position state error estimates are in local geodetic frame) and R_l^e is

the transformation matrix from ENU to ECEF frame (as the velocity state error estimates are in ENU frame). $M_{3\times3}$ is given by Equation (2.35),

$$M_{3\times3} = \begin{pmatrix} -(R_N + h)\sin\varphi\cos\lambda & -(R_N + h)\cos\varphi\sin\lambda & \cos\varphi c\,\mathrm{os}\,\lambda \\ -(R_N + h)\sin\varphi\sin\lambda & (R_N + h)\cos\varphi\cos\lambda & \cos\varphi\sin\lambda \\ 0 & (R_N(1-e^2) + h)\cos\varphi & \sin\varphi \end{pmatrix} \tag{2.35}$$

Equation (2.35) is obtained by linearizing the following equation,

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix}_{ECEF} = \begin{pmatrix} (R_N + h)\cos\varphi\cos\lambda \\ (R_N + h)\cos\varphi\sin\lambda \\ (R_N(1-e^2) + h)\cos\varphi \end{pmatrix} \tag{2.36}$$

where e^2 is obtained using Earth`s average equatorial (a) and polar (b) radius using,

$$e^2 = \frac{a^2 - b^2}{a^2} \tag{2.37}$$

R_l^e is given by,

$$R_l^e = \begin{pmatrix} -\sin\lambda & -\sin\varphi\cos\lambda & \cos\varphi\cos\lambda \\ \cos\lambda & -\sin\varphi\sin\lambda & \cos\varphi\sin\lambda \\ 0 & \cos\varphi & \sin\varphi \end{pmatrix} \tag{2.38}$$

To obtain the process noise covariance matrix Q_{k-1} , we use a numerical integration approach and is expressed as (Petovello, 2003),

$$\mathrm{Q}_k = (\Phi_{k,k-1} G_k \mathrm{q}_c G_k^T \Phi_{k,k-1}^T + G_k \mathrm{Q}_c G_k^T)\frac{\Delta t}{2} \tag{2.39}$$

where q_c represents the power spectral density of the corresponding states. The values of the spectral densities are roughly a guesstimate based on the expected vehicle dynamics (Brown and Hwang 1997). Since the velocity of the chosen vehicular trajectory is approximately constant, the values of the spectral densities are chosen as shown in Table 2.1.

The GPS receiver clock offset is a time-varying error that affects the observations from all the satellites in the same way. The GPS receiver typically uses either a crystal oscillator (XO) or temperature compensated crystal oscillator (TCXO) due to the size and cost constraints in an automotive application. The clock offset and drift error states are modelled as random walk processes over reasonable time span (Brown and Hwang 1997). The spectral density parameters from a standard clock stability model given by,

$$\begin{aligned} q_{c,b_r} &= 2h_0 \\ q_{c,b_d} &= 8\pi^2 h_{-2} \end{aligned} \tag{2.40}$$

where h_0 and h_{-2} are the clock stability parameters that can be obtained from the Allan variance plots of the oscillator used (Brown and Hwang 1997). The GPS receivers used in this research have TCXO clocks and the typical value of the power h_0 and h_{-2} for TCXO are 2e-19 and 2e-20 respectively.

Table 2.1: Power spectral densities for velocity states in GPS-only EKF

Parameter	Power spectral density (m/s/$\sqrt{Hz}$)
East Velocity	2
North Velocity	2
Up Velocity	2

2.4.2.2 GPS/INS Integrated EKF

In order to test the various GPS/INS combinations, GPS and INS observations are processed in an extended discrete time Kalman filter (EKF) implementation. A 23-state EKF is implemented in MATLAB™ to process GPS/INS integrated observations in loose and tight coupling mode. The GPS-only LS and GPS-only EKF were implemented primarily to compare the fault

detection/identification capability whist using GPS observations alone with that of a GPS/INS integrated observations processed in an integrated navigation KF in the presence of single satellite error in GPS observations due to spoofing. The state error vector $\delta \mathrm{x}_k$ GPS/INS EKF used in this research is represented as,

$$\delta \mathrm{x}_k = \begin{pmatrix} \delta r^l & \delta v^l & \delta \varepsilon^l & \delta b_\omega & \delta b_f & \delta S_\omega & \delta S_f & \delta b_r & \delta d_r \end{pmatrix} \tag{2.41}$$

For a tactical grade IMU, the scale factor error remains almost constant, but for lower grade MEMS sensors, it is advisable to have the scale factor error states estimated in EKF. Considering the fact that different grades of sensors were used in this research, and using Equation (2.7), the system state equations and observation equations are established by the combined GPS and INS errors as,

$$\begin{bmatrix} \delta \dot{r}^l \\ \delta \dot{v}^l \\ \delta \dot{\varepsilon}^l \\ \delta \dot{b}_\omega \\ \delta \dot{b}_f \\ \delta \dot{S}_\omega \\ \delta \dot{S}_f \\ \delta \dot{b}_r \\ \delta \dot{d}_r \end{bmatrix} = \begin{bmatrix} D^{-1}\delta v^l \\ R_b^l f^b \varepsilon^l - (2\Omega_{ie}^l + \Omega_{el}^l)\delta v^l - (2\delta\Omega_{ie}^l + \delta\Omega_{el}^l)v^l + \delta g^l + R_b^l b_f + R_b^l f^b S_\omega \\ -\Omega_{il}^l \delta\varepsilon^l - \delta\omega_{il}^l + R_b^l b_\omega + R_b^l \omega^b S_f \\ -\beta_\omega \delta b_\omega + w_d \\ -\beta_f \delta b_f + w_b \\ -\beta_{\omega s} \delta S_\omega + w_{s_\omega} \\ -\beta_{fs} \delta S_f + w_{s_f} \\ \delta b_r + w_{rb} \\ \delta d_r + w_{rd} \end{bmatrix} \tag{2.42}$$

where w_* represents the white noise component of the corresponding state vectors, β_ω, β_f, $\beta_{\omega s}$, β_{fs} are the reciprocal of the time constants for the respective sensor errors, which is the inverse of the correlation time.

The design matrix H_k for the loose coupling EKF is given by Equation (2.43) under the consideration that the GPS receiver outputs the position $(\varphi, \lambda, h)_{GPS}$ in local geodetic frame, velocity $(v_e, v_n, v_u)_{GPS}$ in ENU frame, GPS clock offset (in m) and GPS clock drift (m/s).

$$\mathrm{H}_{k,GPSINSLC} = \begin{pmatrix} I_{6x6} & 0_{6x15} & 0_{6x2} \\ 0_{2x2} & 0_{2x15} & I_{2x2} \end{pmatrix}_{8x23} \tag{2.43}$$

The design matrix H_k for the tight coupling EKF is an extension of Equation (2.34) used in GPS-only EKF with additional 12 sensor error states and 3 attitude error states, and is shown in Equation (2.44) under the consideration that there are *n* GPS pseudorange (in m) and range-rate (in m/s) observations each.

$$\mathrm{H}_{k,GPSINSTC} = \begin{pmatrix} H_{n\times3} \cdot M_{3\times3} & 0_{n\times3} & 0_{n\times15} & 1_{n\times1} & 0_{n\times1} \\ 0_{n\times3} & H_{n\times3} \cdot R_l^e & 0_{n\times15} & 0_{n\times1} & 1_{n\times1} \end{pmatrix}_{n\times23} \tag{2.44}$$

The process noise Q_{k-1} is computed in the similar method as shown in Equation (2.39) and the power spectral densities are same as the ones used in GPS-Only EKF. The spectral density of the process noise is computed based on the Gauss-Markov model parameters used by Godha (2006),

$$\mathrm{q}_{c,b_i} = \sqrt{2\beta_i\sigma_i^2} \tag{2.45}$$

In Equation (2.45), subscript 'i' represents the corresponding sensor error state (ω, f, ωs or fs). The process noise for the MEMS grade sensor errors were considered to be higher than the tactical grade counterparts.

The GPS receiver clock offset and drift are modelled in the same way as specified in section 2.4.2.1 for GPS-only EKF case. In Equation (2.41), the 12 INS sensor error states including the sensor biases and scale factor errors are modelled as first-order Gauss-Markov processes. The Gauss-Markov model parameters are obtained by collecting the raw static data from each of the

IMUs under test for a duration 2.5 hours and computing its auto-correlation function (Gelb 1974) and the parameters used for the various sensor error states are specified in Table 2.2.

Table 2.2: Gauss-Markov Parameters for the modelling sensor errors

INS Grade		Gyro. drift		Accel. bias		Gyro. scale factor		Accel. scale factor	
		$\frac{1}{\beta_\omega}$ (s)	σ_ω (°/h)	$\frac{1}{\beta_f}$ (s)	σ_f (m/s^2)	$\frac{1}{\beta_{\omega s}}$ (s)	$\sigma_{\omega s}$ (PPM)	$\frac{1}{\beta_{fs}}$ (s)	σ_{fs} (PPM)
T	X	6000	0.59	10200	2.8e-4	1500	1000	1500	1000
	Y	3300	0.58	4080	5e-3	1500	1000	1500	1000
	Z	5040	0.69	9120	6.9e-4	1500	1000	1500	1000
MH	X	980	90.06	927	0.002	9000	5000	9000	5000
	Y	975	110.64	910	0.001	9000	5000	9000	5000
	Z	1097	100.31	954	0.003	9000	5000	9000	5000
ML	X	382	211.06	227	0.007	18000	10000	18000	10000
	Y	375	204.64	210	0.007	18000	10000	18000	10000
	Z	297	161.31	364	0.009	18000	10000	18000	10000

2.5 Hypothesis Testing

The equations given in the section 2.4 deal with the estimation of the unknown states x_k or state errors $\delta\mathrm{x}_k$ using a set of observations, either GPS only or both GPS and INS observations. The dispersion in these estimators can be measured using their variances and covariance (Steeves 1987). Hypothesis testing is a mechanism to check the quality of the observations using the information available in the estimated states. It deals with accepting or rejecting a hypothesis under a given error probability. The hypothesis are formulated as linear function of unknown parameters (Koch 1987). The testing process can be broadly classified as fault detection, fault identification and model adaptation. In both fault detection and identification, the residuals/innovations will be

used as a tool for assessing the integrity of the final state estimate. The parameter under test is usually the residual vector (in case of LS shown in Equation (2.21)) or the innovation sequence (in case of KF shown in Equation (2.30)) and it is assumed that the measurement errors are normally distributed as the statistical tests inherently require a known/assumed distribution.

2.5.1 Fault Detection

Fault detection can be termed as a global test on residuals/innovation vector, where all the residuals are tested together. The sum of squares of the residuals weighted by the measurement VCM R_k is used as the test statistic used for the null hypothesis H_0. It can be expressed as,

$$\xi\big|_{H_0} = r_k^T R_k^{-1} r_k \sim \chi^2(\mathrm{n}_k - \mathrm{m}_k) \tag{2.46}$$

For Gaussian measurement errors, the above test statistic follows a χ^2 distribution with (n_k - m_k) degrees of freedom, where n_k is the number of observations and m_k is the number of states. The two-tailed test for accepting a null-hypothesis with a significance level α is given by (Steeves 1987),

$$\chi^2_{\alpha/2} > \xi > \chi^2_{1-\alpha/2} \tag{2.47}$$

If the above condition fails on the low side, then the given measurement variance is probably too large resulting in a small weighted sum. While if it fails on the high side then either the measurement variance is too small or it indicates a presence of one or many outliers in the given set of observations. Subsequently, further tests are conducted as described in fault identification section below to identify the outlier measurement individually.

2.5.2 Fault Identification

Fault detection mainly provides only an indication of presence/absence of an outlier. The overall fault can be due to one or many observations that were available. In order to identify which of the observations are faulty, a local test on each observation is performed.

In both LS and EKF case, the null hypothesis H_0 is considered as the residual vector r_k normalized by its variance $\mathrm{C}_{\mathrm{r}_k}$ follows a standard normal distribution. Therefore, the test statistic for the i^{th} observation is given by,

$$\xi_i\big|_{H_0} = \frac{\left(\mathrm{r}_k\right)_i}{\sqrt{\left(\mathrm{C}_{\mathrm{r}_k}\right)_{ii}}} \sim N(0,1) \tag{2.48}$$

The test for accepting the null hypothesis is given by (Steeves 1987),

$$\left|\xi_i\right| < N_{1-\alpha/2} \tag{2.49}$$

The test is performed for one observation at a time and if a failure occurs, the corresponding observation is identified as an outlier.

2.5.3 Model adaptation

The model adaptation is the process of modifying the estimator based on the fault detection and identification results. It is performed either by rejecting faulty observations or by inflating the corresponding measurement variance R_k. After the adaptation, the innovations and their covariance are computed again, and the tests are repeated. The process of adaptation and re-computation of the test values is repeated until either no failure is detected anymore (reliable solution), until no failure can be identified anymore although a failure is still detected (unreliable solution, flagged), or failure detection and identification is not possible any more (occurs when redundancy is too low, e.g. all redundant observations have been removed) (Wieser et al. 2004). While identifying more than one failure in the course of these iterations, the previously rejected observations may or may not be reintegrated again, once no more failures are detected. Due to the mutual influence of failures on their respective test statistics, a failure may well have been identified erroneously. The methodology of model adaptation is mentioned here to complete the overall process of hypothesis

testing. The results presented in this thesis were restricted to fault detection and identification during a spoofing attack.

The following chapter presents the statistical reliability analysis focussing on estimating the theoretical limits of the blunder detection capability of the various systems under test.

Chapter Three: STATISTICAL RELIABILITY ANALYSIS

Prior to the experimental analysis of the spoofing fault detection/identification performance of these, a statistical reliability analysis of all these GPS and INS sensors used for a typical land vehicular scenario is made to obtain the theoretical limits of the fault detection capability. The internal reliability analysis provides an estimate of the minimum blunder that can be detected in a GPS observation. In the context of this thesis, a blunder/fault is caused due to the spoofing error. The results of this covariance analysis are then used in Chapter Four to design experiments to test the systems on hand. This chapter reviews the general internal reliability equations used and then presents covariance analysis results of the estimated MDB values for a chosen vehicular trajectory using several different systems.

3.1 Statistical Reliability Analysis

In the context of this thesis, statistical reliability is a measure of quantifying the magnitude of blunders that can be detected. It refers to the ability to identify blunders and the impact of an undetected blunder in the state estimates. This provides a reliability assessment of the estimated solution. Statistical reliability is classified into two categories; *internal reliability* and *external reliability*. Internal reliability quantifies the smallest blunder that can be detected on each observation. This is the Minimum Detectable Blunder (MDB). External reliability quantifies the effect of such a blunder when it occurs on the estimated states (Baarda 1968, Baarda 1967).

Before proceeding further with the analysis, it is necessary to state the additional assumptions made. Recalling the review of the estimation methods presented in Chapter Two, no assumptions were made regarding the distribution of the measurement errors. Since the statistical testing inherently requires a known/assumed distribution, the following assumptions were made:

- The measurement errors are normally distributed.

- Only a single blunder occurs at a time. Though this may not be correct in certain applications, this assumption is valid for local test of each innovation presented in this thesis.

The following subsections present the equations used for MDB computation in the LS and EKF estimators.

3.1.1 GPS-only LS

In GPS only LS based estimation, the MDB for the i^{th} observation is given by (Baarda 1968, Baarda 1967),

$$\nabla_{\mathrm{MDB}_i} = \frac{\left(\mathrm{R}_k\right)_{ii}}{\sqrt{\left(\mathrm{C}_{\mathrm{r}_k}\right)_{ii}}}\delta_0 \tag{3.1}$$

As inferred from the above equation, the quantification of MDB is based on the following parameters on an epoch-by-epoch basis:

- Measurement VCM (R_k): The number of GPS observations and its precision play a significant role in the magnitude of MDB. The measurement quality of GPS sensor is directly proportional to the MDB. In other words, a good quality GPS receiver provides a better MDB performance metric. Also, MDB values are low when there are more number of observations available. The redundancy in the observations aids the capability of the fault detector.
- The relative measurement geometry (H_k) between the satellite and the receiver. The value of MDB changes whenever there is a significant change in the measurement geometry. When the user is static, changes in the measurement geometry will not be significant for short time duration unless a satellite gets included or excluded due to visibility. This may not be true in a dynamic user scenario, where the change in measurement geometry happens

more often based on the user motion. For the simulation in this research, a reasonably good satellite geometry was chosen as shown in Figure 3.1.

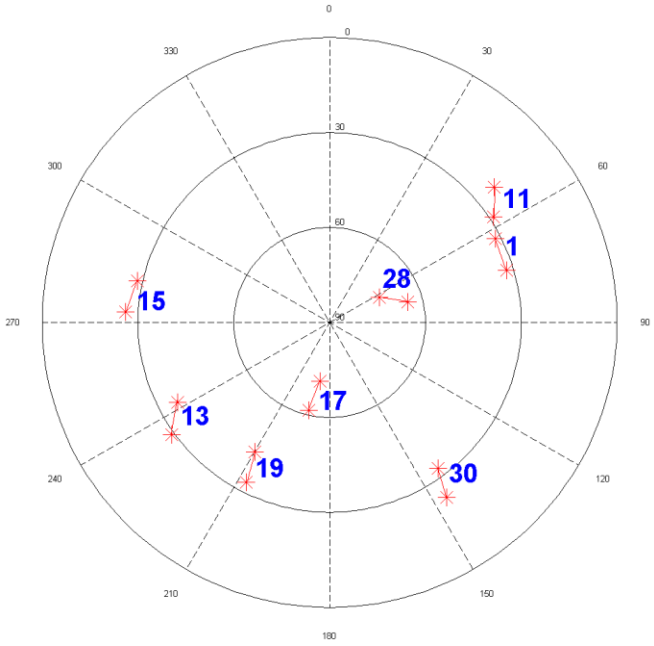

Figure 3.1: Sky plot during the test duration

- Non-centrality parameter (δ_0): A Type-I error is when the null hypothesis H_0 is incorrectly rejected with a probability of α (probability of false alarm). A Type-II error is when the null hypothesis is incorrectly accepted with a probability of β (probability of missed detection). The value of α of 0.1% and β of 10% were adopted from Wieser et al. (2004), where the reliability analysis was done for a high accuracy kinematic positioning. This means that 99.9% of the good observations are accepted while allowing 10% of bad observations into the solution, which gives a non-centrality parameter of 4.57 with respect to Equation (3.2) (Koch 1987).

$$\delta_0 = N_{1-\alpha/2} + N_{1-\beta} \tag{3.2}$$

3.1.2 GPS/INS Integration EKF

In a GPS/INS EKF estimation, the equation for the MDB of the GNSS observations for both loose and tight integration strategies is same and is given by,

$$\left|\nabla_{\mathrm{MDB}_i}\right| = \frac{\delta_0}{\sqrt{\left(\mathrm{C}_{v_k}^{-1}\right)_{ii}}} \tag{3.3}$$

The GPS-only EKF also follows the same Equation (3.3) for the MDB computation except that only GPS observations were used in this case. In case of GPS/INS integrated system, since additional sensor observations were used in a single integrated navigation EKF, the MDB value further depends on the following parameters:

- Choice of the state space model: A larger number of states results in higher MDBs because more of the observations are required to observe these additional states. For a typical automotive application, a low quality sensor is used which requires adding more sensor error states to the navigation EKF.
- Measurement VCM (R_k): The number of additional sensors and their precision decreases the MDB values due to the redundancy in the available observations. Using a tactical grade or a MEMS grade sensor provides same level of redundancy, but different levels of precision that has an impact on the MDB values. The level of this impact is investigated in this covariance analysis.
- Process noise (Q_k): The uncertainty in the dynamics model is directly proportional to the MDB values. Lower the process noise, better the MDB. In order to counter the uncertainties in the vehicle's unpredictable dynamics, higher derivatives of the position states are required to be estimated, but this has a detrimental effect in the MDB values. The chosen

vehicular trajectory for the covariance analysis is a simple motion trajectory and hence only the first derivative of the position is estimated.

- Sample rate of sensors: In order to maintain a common platform for comparison, a 1 Hz update rate is chosen for all GPS/INS combinations. This is low for a typical GPS/INS integration, however it is appropriate and commonly available in an automotive and a handheld pedestrian applications. Also, lower update rate does help reducing the cost and power consumption of the sensors, which is a primary requirement for most of the commercial applications.

3.2 Loose and Tight Coupling Comparison

Recalling the primary difference between loose and tight coupling, which is the number of filters/estimators used. In loose coupling, GPS observations were processed separately using a GPS-only LS/KF estimator followed by a navigation KF, whereas in a tightly coupled system, one common navigation KF is used to process the GPS and INS observations as shown in Figure 2.1. The point to be noted here is that the fault can occur only in the raw GPS observations and can enter the system before the first filter/estimator (Petovello 2003). The first estimator in case of loose coupling is the GPS-only estimator and the internal reliability analysis corresponds to the GPS only filter/estimator. But, the external reliability is always presented for the final integrated GPS/INS LC solution. In tight coupling, the navigation filter uses the GPS observations directly in a single KF, and so the internal reliability of this common navigation filter is investigated.

3.3 GPS/INS Combinations

The covariance analysis is useful in evaluating the smallest magnitude of blunder that can be detected allowing an accepted level of Type-I and Type–II errors. In order to perform the

covariance analysis, a typical vehicular motion reference trajectory as shown in Figure 3.2 was chosen.

Figure 3.2: Reference trajectory (Google Earth image)

The experimental setup used in this research consists of the following grades of GPS receiver and IMUs:

- Navigation grade GPS receiver (N)
- Automotive grade GPS receiver (A)
- Smartphone grade GPS (M)
- Tactical grade IMU (T)
- Automotive MEMS high-grade IMU (MH)
- Smartphone MEMS low-grade IMU (ML)

The initial R_k and Q_k is chosen based on the GPS-IMU combination with respect to their specifications shown in Table 3.1.

.

Table 3.1: GPS receiver and IMU specifications

GPS	Parameter	Value
Navigation (N)	Position STD (RMS)	± 1.2 m
	Velocity STD (RMS)	± 0.2 m/s
Automotive (A)	Position STD (RMS)	± 3 m
	Velocity STD (RMS)	± 0.4 m/s
Smartphone (M)	Position STD (RMS)	± 10 m
	Velocity STD (RMS)	± 1 m/s
IMU	**Parameter**	**Value**
Tactical (T)	Accelerometer bias	0.5 mg
	Accelerometer white noise	40 μg/√Hz
	Gyro drift	0.3°/hr
	Gyro white noise	0.001 °/sec /√Hz
Automotive MEMS (MH)	Accelerometer bias	16 mg
	Accelerometer white noise	60 μg/√Hz
	Gyro bias	12°/hr
	Gyro white noise	0.01 °/sec /√Hz
Smartphone MEMS (ML)	Accelerometer bias	50 mg
	Accelerometer white noise	218 μg/√Hz
	Gyro bias	36°/hr
	Gyro white noise	0.03 °/sec /√Hz

3.4 Results

In this covariance analysis, it is assumed that the IMU sensor errors are calibrated and a good initial estimate of the state vector with a position accuracy of <0.1 m and a velocity accuracy <0.001 m/s is known a priori.

3.4.1 N-grade GPS with T and MH-grade IMU

Figure 3.3 shows the MDB plot of the GPS range observations with respect to 8 visible satellites from the chosen vehicular motion trajectory for the navigation grade (N) GPS receiver in the following modes:

- N-grade GPS-only using LS estimator – N (LS) (subplot 1)
- N-grade GPS-only using EKF estimator – N (KF) (subplot 2)
- N-grade GPS tight-coupled with T-grade IMU – N-T (subplot 3)
- N-grade GPS tight-coupled with MH-grade IMU – N-MH (subplot 4)

In case of stand-alone GPS, MDB depends only on the GPS receiver measurement accuracy R_k. So the N-grade GPS receiver is expected to provide a better MDB value compared to A and M-grade receivers. The satellite-receiver observation geometry H_k also plays a role in the magnitude and changes that can impact the estimated MDB. In order to mimic a close to real data scenario, the variation in the satellite visibility (accounting for the blockages due to buildings and foliage) for the given trajectory was recorded using one of the GPS receivers and replayed to form the covariance simulation. The satellites were chosen based on the visibility data taken during the trial run. The number of GPS observations n_k used at every k is 8, 7, 6 or 5 as shown in Figure 3.4.

It can be observed that whenever there is a change in the number of observations, the value of MDB changes. The vehicle during the trial run was kept static for the first 280 s and MDB remains approximately constant with slight variation only due to small changes in the satellite geometry.

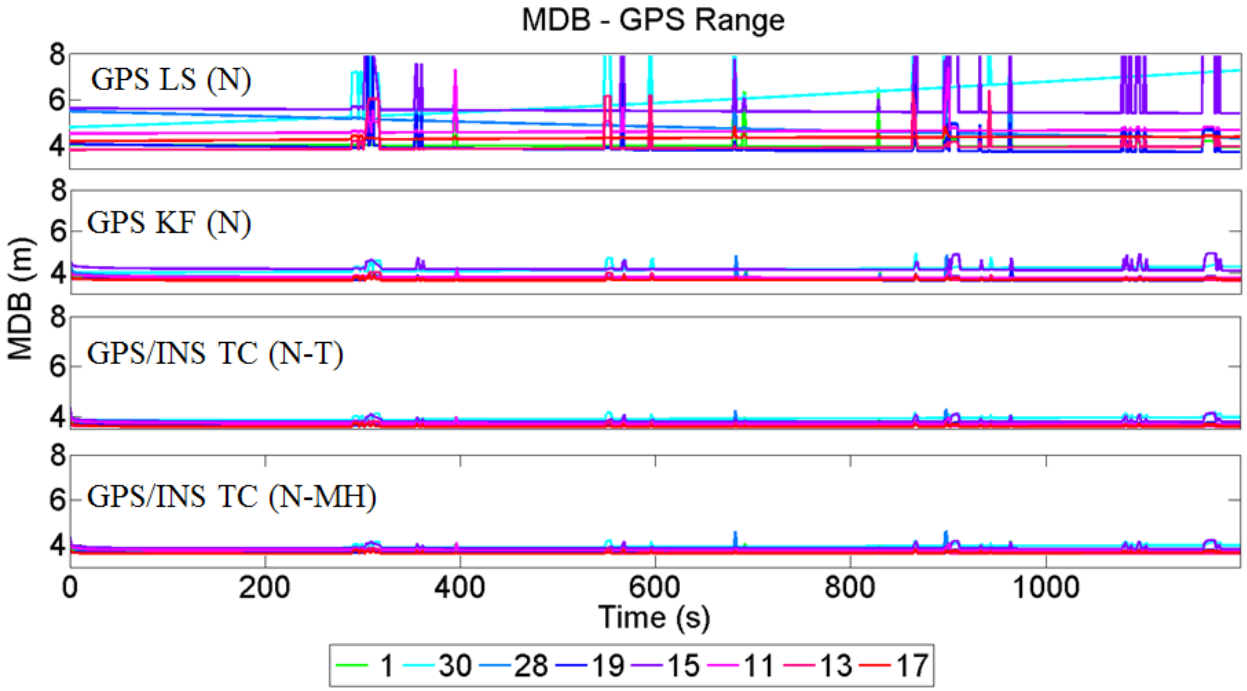

Figure 3.3: MDB values for GPS range observations using N-T combination

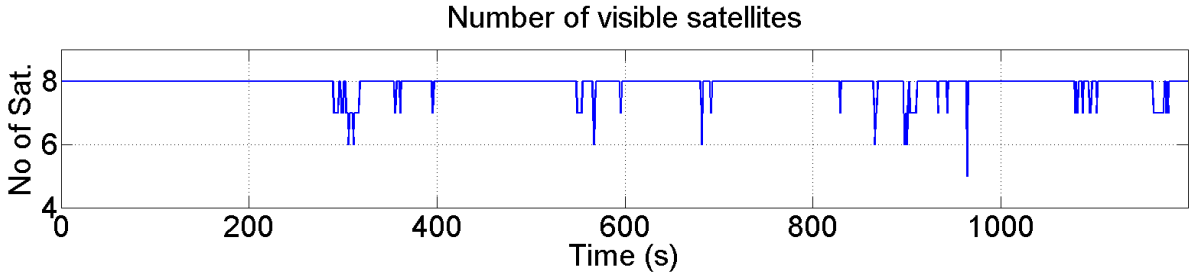

Figure 3.4: Number of visible satellites

When the vehicle is static, there exists no significant change in the measurement geometry for short duration and hence the MDB values purely depend on the sensor quality of GPS and IMUs used. When the vehicle starts moving, the measurement geometry H_k changes due to vehicular motion as well as the satellite visibility. Therefore, a more variations were observed in the MDB plot commensurate to the changes in the satellite visibility. Satellite PRN 30 is a falling satellite as inferred from the sky plot shown in Figure 3.1, and hence the MDB estimates for this satellite tends to increase in epoch-by-epoch LS estimation. Though the same behaviour was

observed in other cases as well for satellite PRN 30, due to the filtering effect of the EKF estimator, the variation in MDB is less.

When GPS observations are integrated with T-grade INS, the number of states to be estimated increases accounting for the IMU sensor errors states. Though this would mean a worse MDB, the magnitude of the impact depends on the sensor quality used. Unlike GPS-LS, the VCM of GPS/INS integrated EKF state estimates depends on $P_k^{(-)}$ and the system model uncertainty Q_k. So the variation in MDB values in the EKF is much smoother and less compared to the LS case. Also, additional observations from the IMUs provide a better $P_k^{(-)}$, and thus a relatively lower MDB. This gives a slight improvement in the MDB performance as compared to using GPS-only EKF estimator.

Note that the INS quality in N-T case is very good and hence this improvement is more evident. To understand the behaviour of comparatively poor quality INS, the test was repeated using MH-grade INS integrated with the N-grade GPS (N-MH combination), and as observed from Figure 3.3, the MDB values were less than the GPS-only case, but slightly higher than the N-T combination. This increase in the MDB compared to N-T combination is solely due to the poor INS sensor quality and a reasonably higher Q_k.

Figure 3.5 shows the similar MDB values of the GPS range-rate observations, providing a theoretical estimate of the minimum range-rate (Doppler) error that can be detected. A similar MDB performance observed for the range-rate observations as well with respect to the vehicular motion. When there is change in vehicular dynamics and/or the measurement geometry, the MDB values tend to vary.

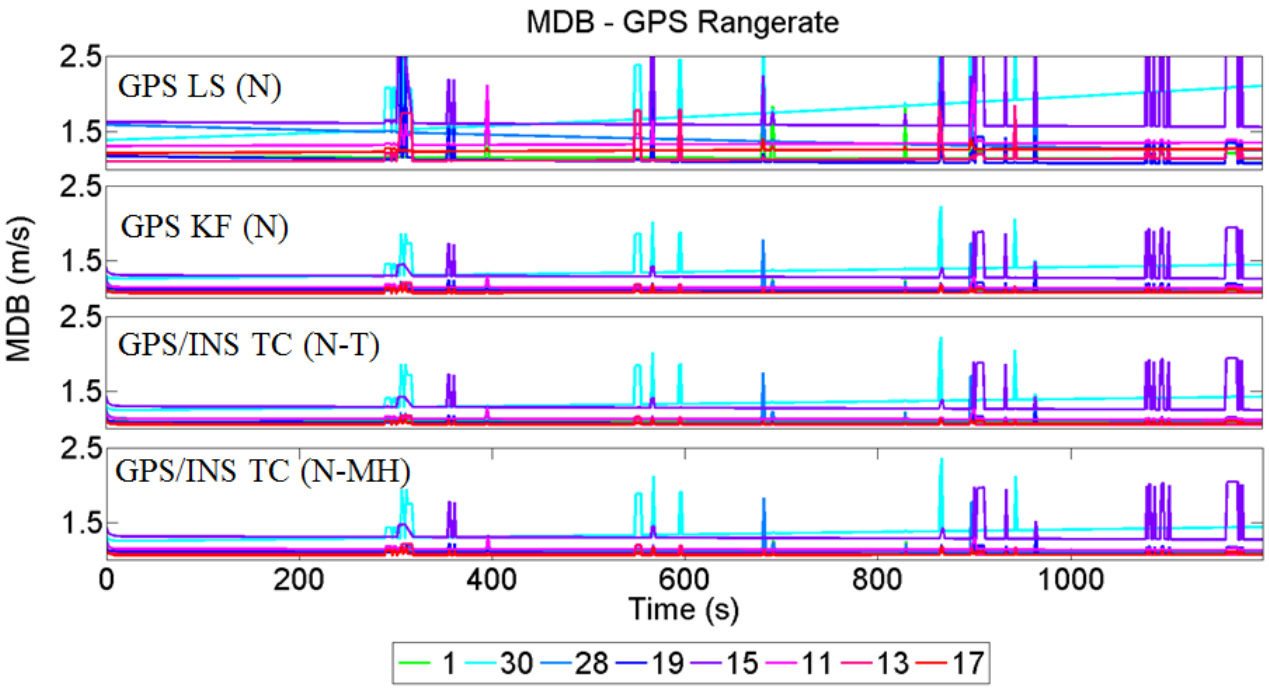

Figure 3.5: MDB values for GPS range-rate observations using N, N-T, and N-MH combinations

3.4.2 A-grade GPS with T, MH and ML-grade IMU

The covariance analysis is repeated for the other GPS/INS combinations considering the same number of GPS observations are available in each case. Figure 3.6 and Figure 3.7 shows the MDB values for GPS range and range-rate measurements respectively for the A-grade GPS in the following modes:

- A-grade GPS-only using LS estimator – A (LS) (subplot 1)
- A-grade GPS-only using EKF estimator – A (KF) (subplot 2)
- A-grade GPS tight-coupled with T-grade IMU – A-T (subplot 3)
- A-grade GPS tight-coupled with MH-grade IMU – A-MH (subplot 4)
- A-grade GPS tight-coupled with ML-grade IMU – A-ML (subplot 5)

The value of MDB increased commensurate to the increase in R_k compared to the N-grade receiver combinations. In addition to T and MH-grade INS integration, a smartphone grade MEMS sensor (ML) integration is also considered. This is done to investigate the impact of MDB caused by a low-cost MEMS sensor on a relatively good GPS good automotive GPS receiver. As inferred from Figure 3.6, integration of a ML-grade sensor worsens the fault-detection/identification capability of the system especially when there are less number of GPS observations available. The variations in MDB changes are more significant in using A-ML combinations compared to the A-T and A-MH combinations. The higher R_k of the GPS observations also adds to the fact that a spoofing range error of less magnitude might go undetected whilst using A-ML combination.

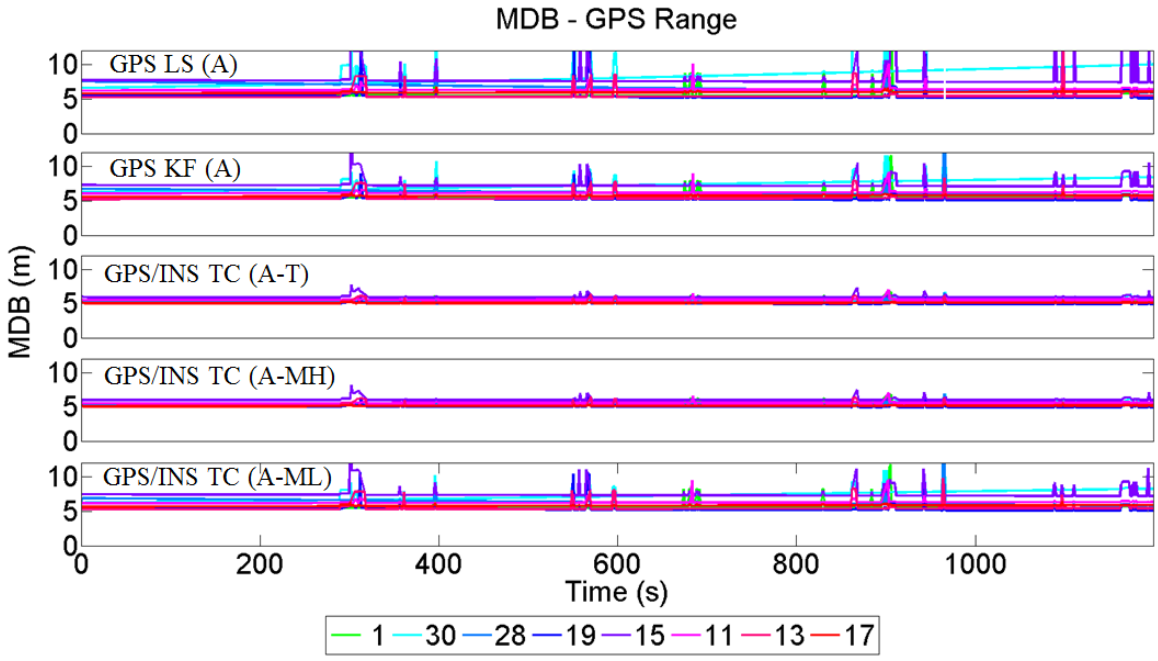

Figure 3.6: MDB values for GPS range observations using A, A-T, A-MH and A-ML combinations

The Doppler error MDB represented as the range-rate error (in m/s) follows the same pattern as the range MDBs, and the plot is shown in Figure 3.7. As observed in the range MDB case, the A-ML combination shows a poor fault-detection performance amongst the three GPS/INS

combinations. This is primarily driven the poor IMU quality due to a higher system model uncertainty of the IMU sensor error states.

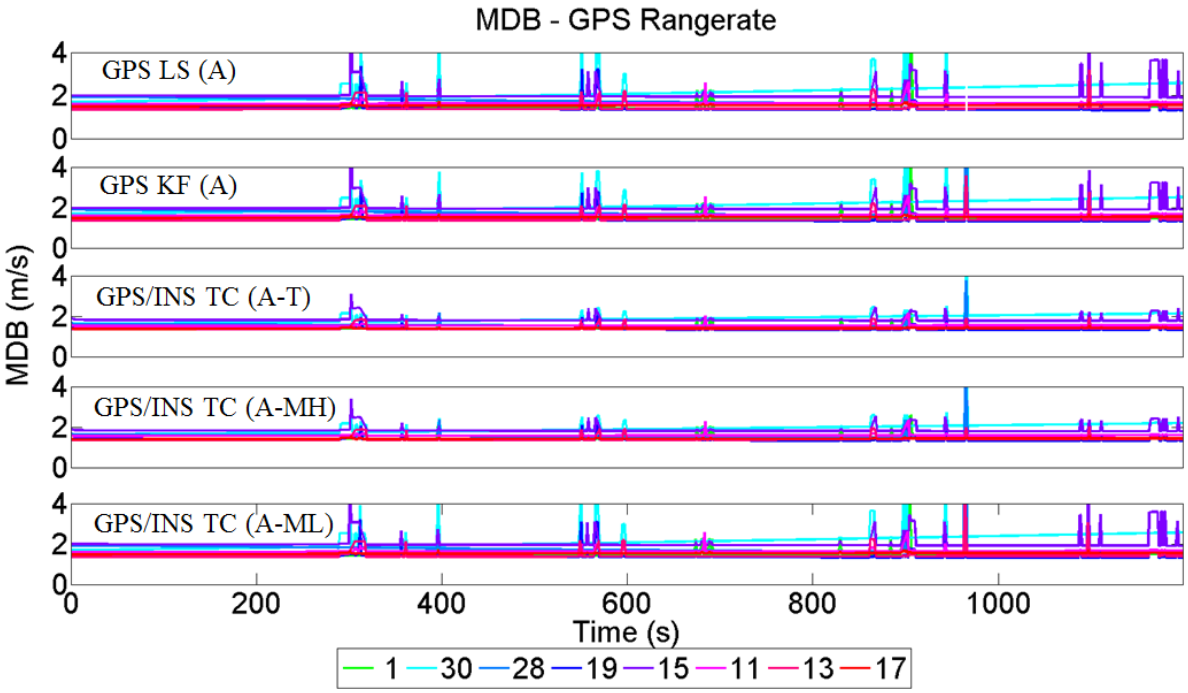

Figure 3.7: MDB values for GPS range-rate observations using A, A-T, A-MH and A-ML combinations

3.4.3 M-grade GPS with ML-grade IMU

The final set of test systems considered is using a smartphone M-grade GPS in the following modes:

- M-grade GPS-only using LS estimator – M (LS) (subplot 1)
- M-grade GPS-only using EKF estimator – M (KF) (subplot 2)
- M-grade GPS tightly-coupled with ML-grade IMU – M-ML (subplot 3)

Figure 3.8 and Figure 3.9 shows the MDB plot for the GPS pseudorange and range-rate observations respectively for all the above mentioned combinations.

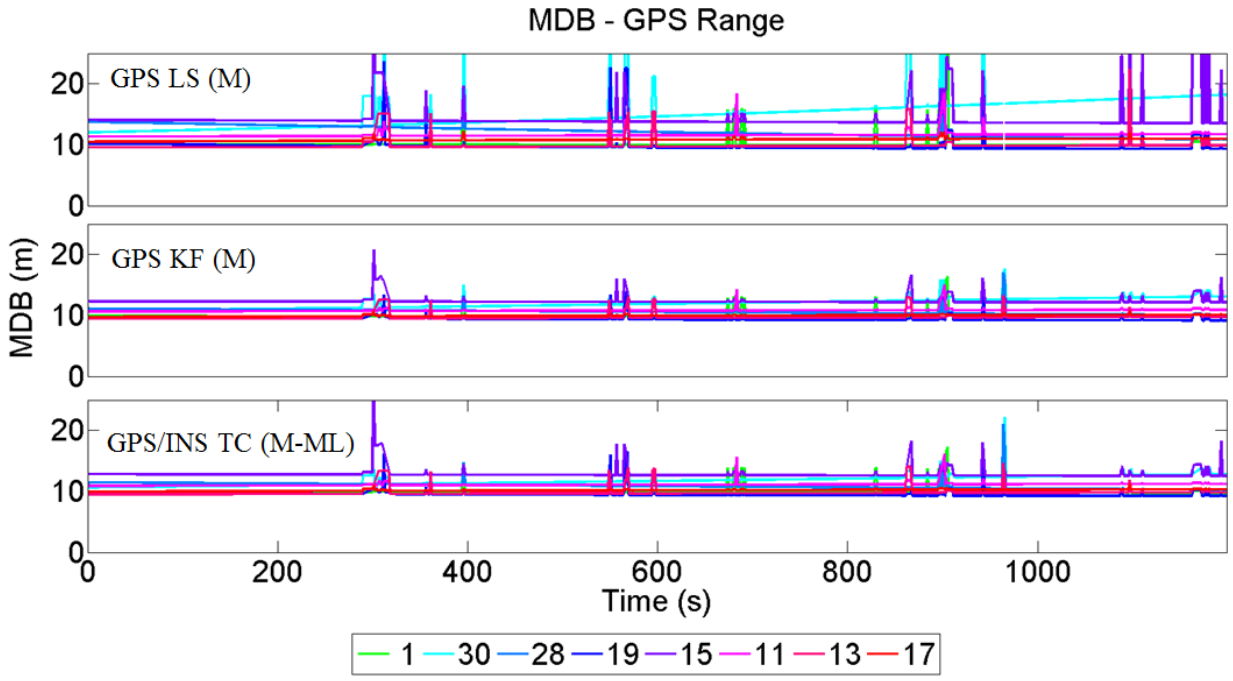

Figure 3.8: MDB values for GPS range observations using M and A-ML combinations

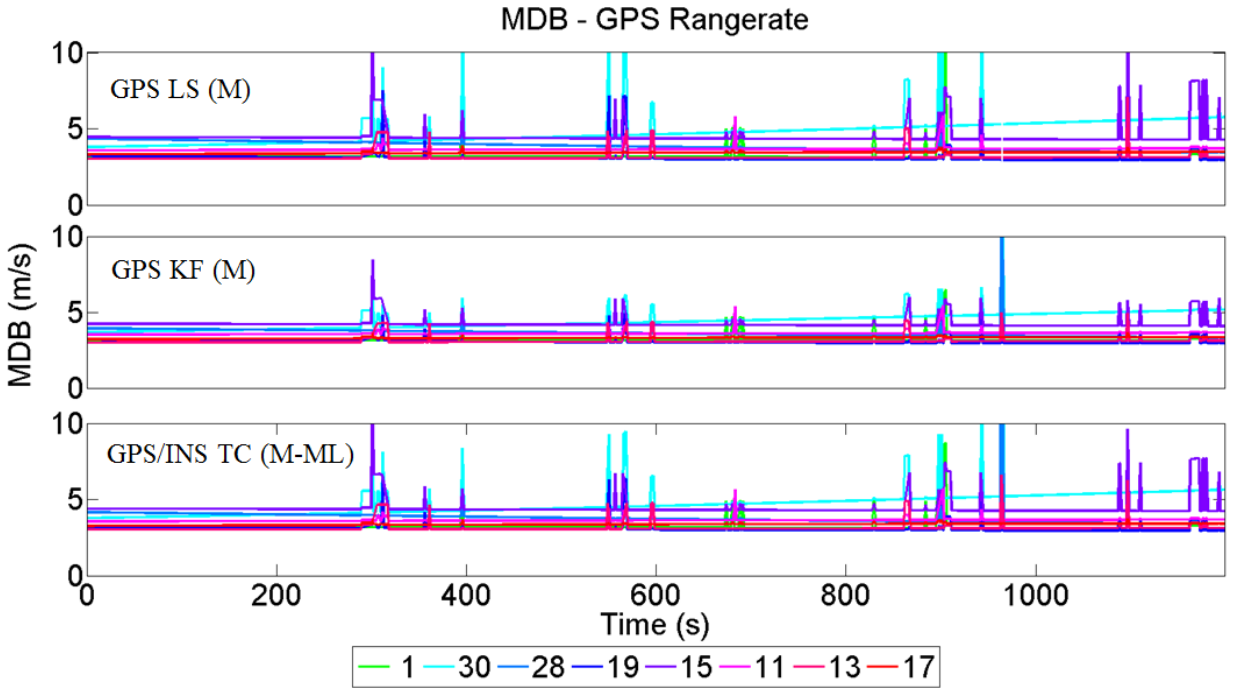

Figure 3.9: MDB values for GPS range-rate observations using M and M-ML combinations

It is clearly evident that the fault-detection performance is worse in this case compared to the higher grade GPS or GPS/INS combinations. Moreover, integrating a poor grade sensor, increases the uncertainty of the sensor error estimates in the system model and thus has a higher process noise. This certainly has a detrimental impact on the MDB values in the integrated M-ML system. The covariance analysis results show that the MDB values in using M-grade GPS in a stand-alone EKF estimator is less than the M-ML integrated system on time epochs where we have less GPS measurements available. This was observed in the A-ML combination as well, and it becomes increasingly difficult to identify faults in GPS measurements using a poor grade sensor.

3.5 Summary

To summarize the results and have a statistical comparison across the different systems considered, the root-mean-squared (RMS) value of the MDB for range and range-rate measurements are computed and presented as a bar chart in Figure 3.10. The GPS-only results are shown for N, A and M-grade receivers using both LS and EKF estimators. The MDB is primarily a function of GPS receiver measurement accuracy (R_k). If the receiver measurement noise is higher, it is difficult to detect a fault. Covariance analysis show that integrating even a tactical grade IMU with an automotive grade GPS receiver, does not give any advantage in terms of MDB performance. Using the same quality inertial sensors integrated with two different grades of GPS receiver, provides different MDB values but mainly as a function of the GPS R_k. For example, Figure 3.10 shows that minimum of ~4 m range error in a single observation can be detected in the N-T combination for satellite PRN 30, and the MDB increase to ~12 m range error while using a lower grade combination (M-ML). This same satellite PRN will be used for the single satellite spoofing error in the experimental analysis using actual observation presented in the next chapter.

The RMS values for range MDB for satellite PRN 30 for the entire simulation duration is listed in Table 3.2.

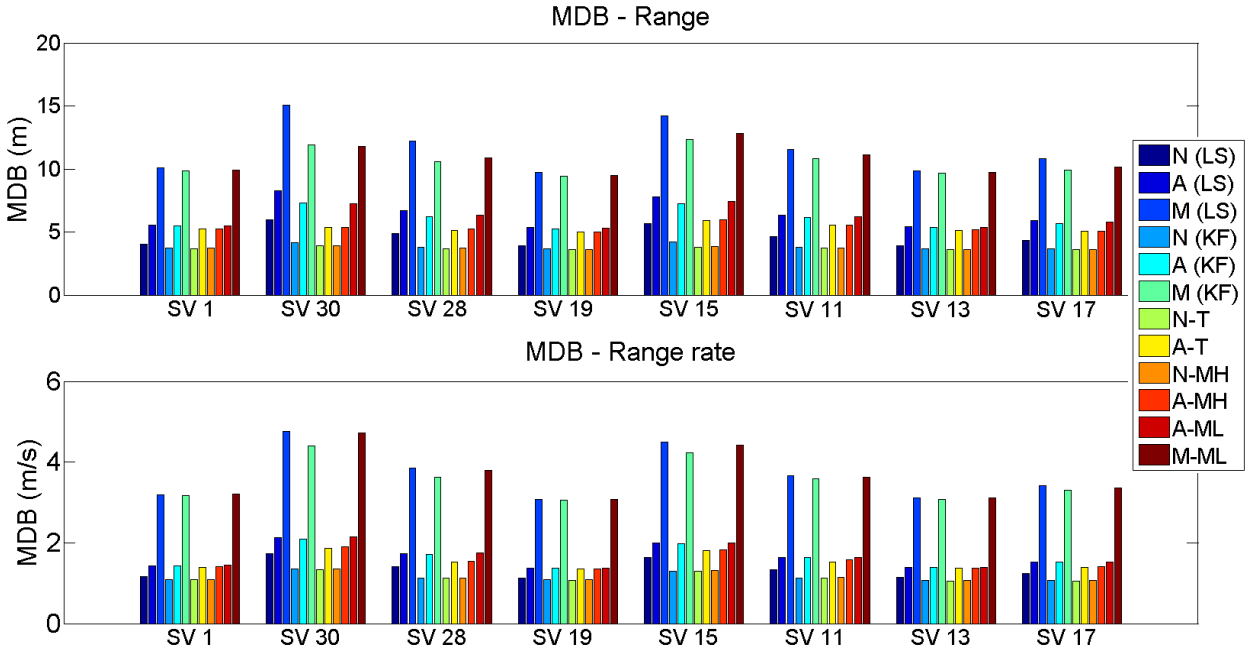

Figure 3.10: Comparison of MDB values for different GPS/INS combination

Table 3.2: GPS range MDB for satellite PRN 30

GPS/IMU	GPS Range MDB for satellite 30 (m)
N (LS)	5.993
A (LS)	8.244
M (LS)	15.057
N (EKF)	4.152
A (EKF)	7.297
M (EKF)	11.938
N-T	3.898
A-T	5.349
N-MH	3.905
A-MH	5.360
A-ML	7.217
M-ML	11.764

Amongst the GPS/INS combinations used, the N-T combination provides the best fault-detection performance in terms of MDB and M-ML shows the least. But still using the M-ML combination does have slight advantage in single satellite spoofing detection over using M-grade GPS in the stand alone case, especially in conditions where there are more good GPS observations available.

Having analysed and presented the theoretical limits of MDB for the GPS observations using statistical internal reliability analysis, the following chapter presents the results of the spoofing detection capability using actual data from the GPS/INS systems.

Chapter Four: EXPERIMENTAL RESULTS

The covariance analysis from the previous chapter provided an estimate of the MDB of the GPS observations. To validate the simulation results, actual GPS and INS data, for each GPS/INS combination is collected in a suburban road environment. In order to emulate spoofing, measurement errors (i.e. errors in pseudorange and Doppler with respect to a spoofing trajectory) were added during post-processing for a specific time duration. The magnitude of errors, the rate, and the duration of the error injection were chosen based on the theoretical limits obtained from the covariance simulation. This chapter presents the details regarding the experimental data collection setup, spoofing simulation and the fault detection/identification results of the various GPS/INS combinations.

4.1 Experimental Setup

The experimental setup used for data collection is shown in Figure 4.8. The GPS antennas and the IMUs were rigidly mounted on top of the vehicle and authentic data was collected from all the GPS receivers and IMUs mentioned above. Two separate GPS antennas were used for the different receivers under test to maintain a reasonable good signal strength. The corresponding lever arm offsets were noted down, which will then be used to do the necessary corrections in post-processing and the details are shown in section 4.2. In order to provide a fair comparison across different receiver combination, observations from the satellites that are common to both the antennas were only used for processing. The sky plot of the GPS satellites used is shown in Figure 3.1. The satellites were chosen such that the corresponding observations were available to all the three GPS receivers under test. The vehicle was driven in the same trajectory used for the covariance simulation. To aid the filter convergence for the sensor error estimates, a random motion of figure of eight is performed prior to the actual data collection window. All IMUs used

were calibrated before the start of the data collection window. The EKF includes the estimation of the bias and scale factor error corrections of accelerometers and gyroscopes to aid continuous calibration of the IMUs.

In post-processing, the GPS observations from the N, A and M-grade receivers were processed using an epoch-by-epoch single point LS and an EKF algorithm implemented in MATLAB™ to obtain the GPS stand-alone state estimates. A loose and tight-coupled navigation Kalman filter was implemented to process the combined GPS and INS observations. The software was made configurable to process observations from any of the GPS and IMU systems, based on the GPS-INS combination required.

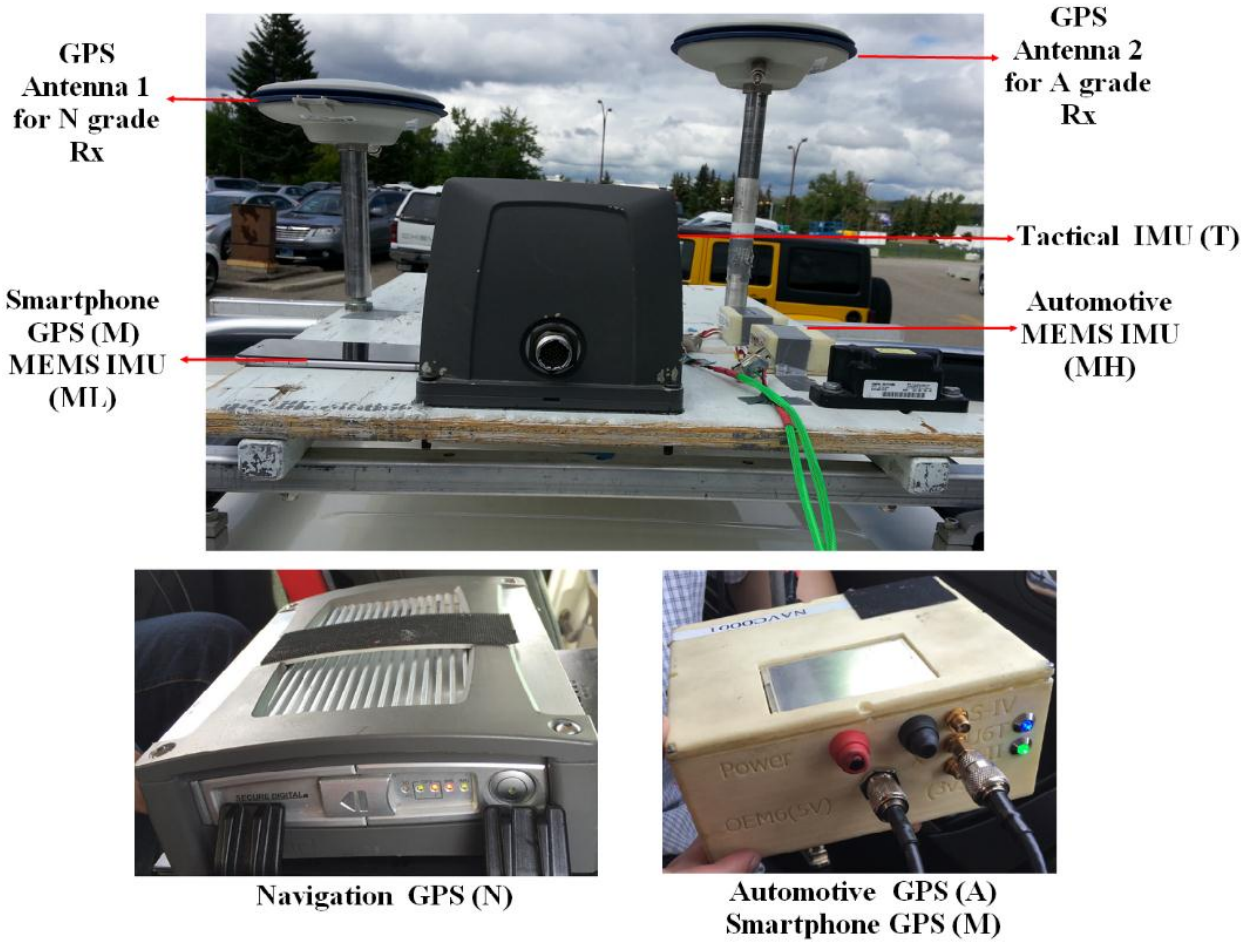

Figure 4-1: Data collection setup

Data was collected in a reasonably open sky in the suburban region of Calgary, Canada. A NovAtel™ SPAN SE and LCI IMU logged data was processed using the NovAtel's Inertial Explorer™ software in dual-frequency RTK mode with forward and backward smoothing to provide a sub-decimeter reference trajectory (shown in Figure 3.2).

The experimental dataset was collected with a navigation grade GPS receiver (N), automotive grade GPS receiver (A), a smartphone equivalent GPS chipset module (M) and smartphone. Typically, the automotive grade GPS module can also be considered as a smartphone grade GPS, but the hardware involved in smartphone antenna are worse than the ones used for automotive navigation (for example, usage of poor antenna in smartphone causes more measurement errors). GPS position data from smartphone was logged, but there was no provision to log the pseudorange and Doppler observations from the GPS module used in a smartphone as they are not the standard outputs. Hence, actual GPS observations from the smartphone could not be used for analysis in tight-coupling mode. So observations from a smartphone equivalent GPS chipset, that has similar specifications as that of a smartphone GPS were considered as M-grade GPS observations.

In addition to these GPS receivers, the setup is equipped with various grades of inertial sensors and has a capability to interface to a maximum of 10 external sensors. Raw IMU observations from a tactical grade (T) IMU, an automotive MEMS (MH) IMU, and a smartphone MEMS (ML) IMU was logged. The logged data from all the sensors are synchronized with the GPS observations with respect to the GPS time tag. The post-processing software was implemented to verify and use the measurements from IMU and GPS only with a synchronized time tag event thereby allowing a flexibility to configure different GPS/INS combinations.

4.2 Lever-Arm Compensation

GPS observations made by the GPS receiver corresponds to the phase centre of the GPS antenna, whereas the observations from IMU corresponds to the centre of the three sensitivity axes. These two point are not same and so when the observations from these two systems are combined, this offset needs to compensated. This difference is generally termed as lever-arm offset. Note that there are two GPS antennas used in the experimental setup. GPS antenna-1 was connected to N-grade GPS, and so for N-T and N-MH combinations, the lever-arm offset was noted between the respective IMUs to the phase centre of GPS antenna-1. GPS antenna-2 was connected to A-grade and M-grade GPS, therefore for A-T, A-MH, A-ML and M-ML combinations, the lever-arm offset between the corresponding IMU with respect to GPS antenna-2 was used. Though the offsets between these lever-arms were less than 1m, it is always a good practise to compensate for the lever-arm offset.

Table 4.1: Lever-arm offset vectors in body frame

GPS	T-grade			MH-grade			ML-grade		
	X (m)	Y (m)	Z (m)	X (m)	Y (m)	Z (m)	X(m)	Y (m)	Z (m)
GPS Antenna-1	-0.242	0.205	0.1	-0.120	0	0.15	NA		
GPS Antenna-2	-0.242	-0.205	0.08	-0.120	0.410	0.17	-0.267	0.02	0.18

The lever-arm in b-frame (LA^b) is transformed to LLF using the transformation matrix R_b^l as shown in Equation (4.1) to obtain the lever-arm vector in LLF (LA^l), which is then added to the INS based position estimate using Equation (4.2) (Noureldin et al 2014).

$$LA^l = R_b^l LA^b \tag{4.1}$$

$$\begin{bmatrix} \varphi \\ \lambda \\ h \end{bmatrix}_{LA_{compensated}} = \begin{bmatrix} \varphi \\ \lambda \\ h \end{bmatrix}_{INS} + \begin{bmatrix} \frac{LA_y^l}{R} \\ \frac{LA_x^l}{R\cos\varphi} \\ LA_z^l \end{bmatrix} \tag{4.2}$$

4.3 Spoofing Simulation and Results

Various spoofing threat profiles were generated considering the vehicle dynamics and the spoofing dynamics. In the context of this thesis, the spoofing dynamics are the rate at which errors are introduced into the GNSS observations, which consequently diverts the target receiver from the true position or the true trajectory. The worst-case spoofing fault profile is the one where the faults are injected slowly into the GNSS observations, which can corrupt the INS calibration without being detected.

Radiating spoofing signals in outdoors requires high power amplifiers and permission, which are practically very difficult and hence the spoofing simulation was done during post-processing of the collected datasets. A configurable spoofing software was developed in MATLAB™ to inject faults to selected GPS observations, which includes pseudorange and Doppler. A spoofing profile was first selected and the position and velocity at every epoch of the spoofing trajectory is determined. The range and Doppler measurement errors (causing the fault due to spoofing) commensurate to the position and velocity of the spoofing trajectory are then computed and added to the actual observations. The satellites for which the spoofing faults are to be added are configurable in the software. These faulty observations were then fed to the navigation Kalman filter.

The spoofing generator module shown in Figure 1.3 generates the erroneous pseudorange and range-rate observations for the satellites chosen during spoofing configuration. The position and velocity errors induced due to spoofing fault is configured in ENU frame. The equivalent pseudorange and range-rate biases were obtained by transforming the spoofing trajectory from ENU to ECEF frame and computing the LOS vector with respect to the satellite position and velocity of the respective satellite at every spoofing time epoch.

In order to test the detection limits in lines with the statistical reliability analysis simulation presented in Chapter Three:, four difference spoofing profiles with different spoofing dynamics were selected based on the MDB results obtained from the covariance analysis. For the first three spoofing profiles, spoofing duration was chosen to be 120 s. It is assumed that EKF is running for at least a minute prior to the spoofing start time t_s. The four spoofing profiles with different spoofing dynamics were selected with following configurations:

1. Step east position error of 16 m at the first spoofing epoch t_s with a step velocity error of 0.1 m/s, which provides a slowly changing position error for the spoofing duration t_{sd} of 120 s (Figure 4.1).
2. Step velocity error of 3 m/s at t_s that provides a ramp position error during the entire t_{sd} of 120 s (Figure 4.5).
3. Ramp velocity error starting with 0.1 m/s at t_s with an increment of 0.1 m/s at every epoch. This gives a parabolic change in position errors during t_{sd} of 120 s (Figure 4.6).
4. Ramp velocity error starting with 0.1 m/s at t_s with an increment of 0.2 m/s at every epoch, but for a longer t_{sd} of 180 s (Figure 4.7).

Note that in all the above four profiles, the spoofing error is added to only one satellite (satellite PRN 30) as the comparison is made with GPS LS estimator In an epoch-by-epoch LS estimation,

the previous history of the state vector and its variance were not used for fault detection. If all observations were spoofed, then the LS state vector converges to the spoofed location and the estimator will never be able to detect or identify a fault. It would be more appropriate to use a GPS only KF estimator or a sequential LS to detect faults in such a case. Also, single-satellite spoofing is done to comply with the assumption made for blunder detection, which is only one blunder is present at any given time epoch. However, for the innovation testing in the KF case, the results shown here can be generalized to multiple spoofed satellite case since with innovation testing multiple satellite spoofing faults would also be detected with the same significance level at the first epoch.

4.3.1 Spoofing Profile 1

The first spoofing profile is chosen to provide a sudden step error in the east position with an fault slightly higher than the MDB RMS values obtained from the covariance simulation. An east position bias of 16 m was injected at k = 650 s, that gives an equivalent range observation bias of ~8 m to satellite PRN 30 at t_s. The position, velocity and the equivalent measurement faults added due to spoofing profile 1 are shown in Figure 4.1.

A very high value of a step change in the spoofing fault is easily detectable in all combinations, but in order to test the difference in the chosen GPS and INS sensors, the magnitude of the spoofing error at t_s is chosen to be marginal to the maximum MDB RMS value obtained for all the GPS-INS combinations. The purpose of the test is to verify whether a marginal step change in spoofing fault in a GPS observation can be detected by the estimators or not.

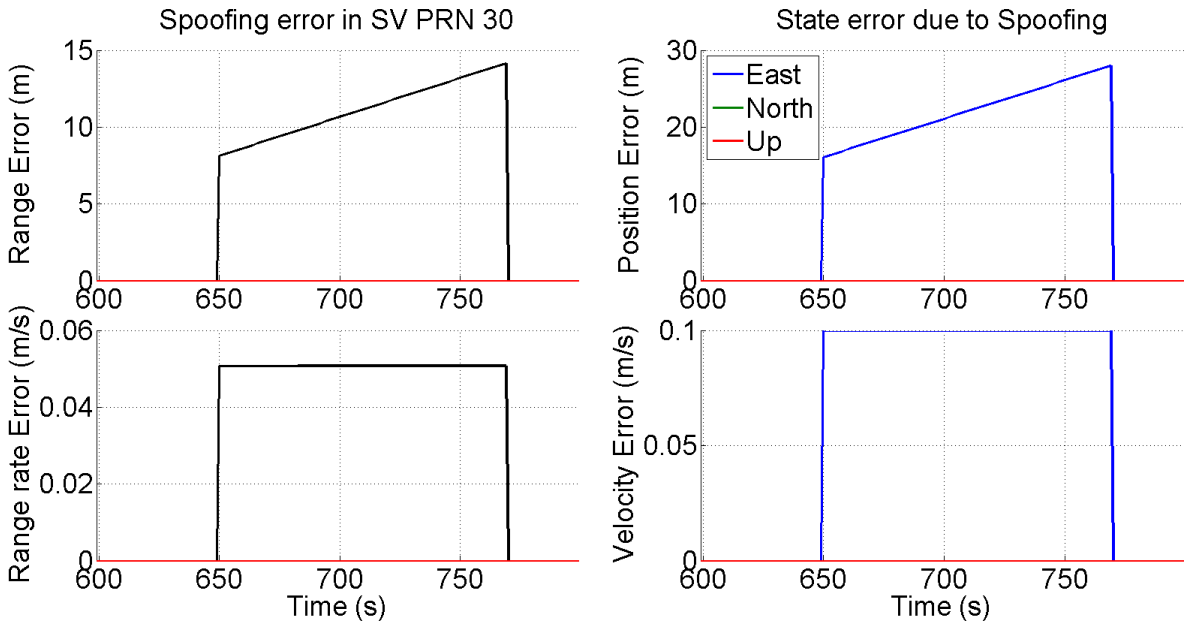

Figure 4.1: Faults due for spoofing profile-1

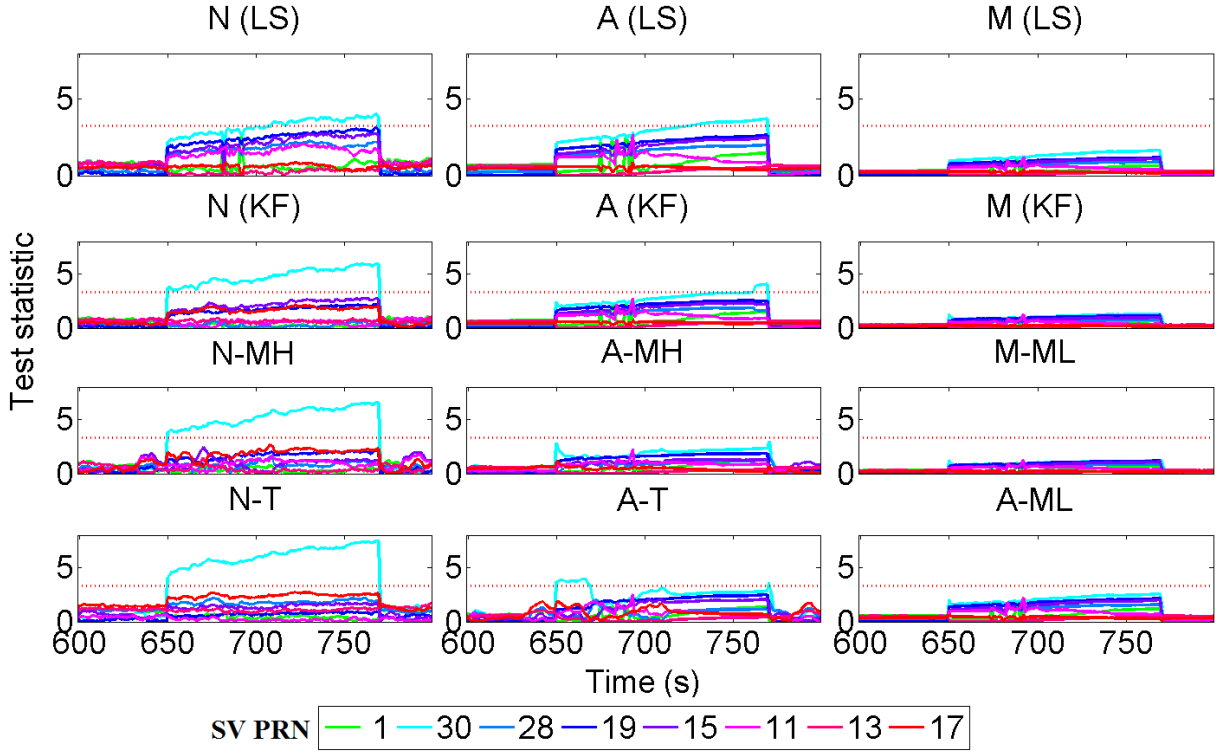

Figure 4.2: Fault identification – Spoofing profile1

The local test statistic of residuals/innovations (method of fault identification) for spoofing profile-1 is shown in Figure 4.2 with a horizontal red dotted line indicating the threshold for

accepting H_0. The horizontal red dotted line indicates the threshold set for outlier detection. Here the outlier is introduced due to the spoofing error being added to the observation and hence this gives an indication of spoofing detection.

If a blunder is detected for an observation from satellite PRN 30 at the first epoch, the observation is rejected from the updating the EKF state estimates Also, the pseudorange and range-rate observations from the same satellite PRN are tested independently. If the pseudorange observation is flagged to be an outlier, the corresponding range-rate observation of the same PRN is not flagged/rejected until a failure is detected in the range-rate observation test statistic. This is done to examine the impact of a small velocity error that can go undetected even when large step error is detected from the same satellite PRN.

4.3.1.1 Epoch-by-epoch LS

The performance of the GPS-only epoch-by-epoch LS estimators is shown in the top three subplots of Figure 4.2. The N-grade and the A-grade GPS receiver failed to identify the faulty GPS observation at the first spoofing epoch t_s and this allowed the error to get included into the overall state estimates. Fault identification takes longer time in A-grade compared to the N-grade GPS. The fault added to the GPS observation due to spoofing in satellite PRN 30 would corrupt the other good observations as well if it is not identified and removed from the observation update at the first spoofing epoch. But during the course of spoofing when the spoofing fault becomes larger, both N-grade and A-grade GPS was able to identify the fault. The M-grade GPS receiver, since the measurement noise is much higher than that of an N-grade GPS and the spoofing error, the detection failed throughout the spoofing duration. This is primarily due to poor GPS receiver measurement quality compared to the magnitude of the spoofing error.

4.3.1.2 GPS-Only EKF

Note that the estimation is based on epoch-by-epoch LS, and each observation at every epoch is assumed to be independent. The history of state estimates is not used in any way during the residual testing of the current epoch. So the next test was performed considering the temporal correlation of the state vectors using an EKF estimator. The three subplots in row 2 of Figure 4.2 shows the innovation testing results for N, A and M-grade GPS receivers processed using GPS-only EKF.

Recalling the primary difference between LS and EKF, the advantage of doing the innovation testing prior the measurement update using the predicted state estimates does have a significant impact on the level of spoofing detection. From Figure 4.2, it is clearly evident that a fault that went undetected whilst using epoch-by-epoch LS in N-grade GPS, got detected at t_s in the EKF innovation testing and was rejected from getting updated into the state estimates thereby not corrupting it. This was not the case for an A-grade GPS, because the spoofing error induced was so marginal to the MDB value and hence went undetected, but it can be observed that the test statistic is close to the threshold where a higher magnitude of spoofing fault could be detected. The fault detection analysis for different magnitudes of spoofing faults presented in section 4.3.1.4. The fault identification performance of M-grade GPS receiver is much worse than the A-grade and in both cases the fault went undetected.

4.3.1.3 GPS/INS Integrated EKF

The next logical step is to investigate the fault identification capability of GPS/INS integrated systems. Since the testing is to identify spoofing fault in individual GPS observation, TC results are presented. As discussed in section 3.2, the fault in an individual GPS observation

can enter the system only on the first filter/estimator, the results of GPS-LS (which is used as the first estimator for GPS/INS LC method in this work) will be the same for GPS/INS LC case.

The subplots titled N-T and N-MH in Figure 4.2 shows the fault identification performance of N-grade GPS/INS combinations. Using N-T combination, the detector is clearly able to identify the outlier at the first epoch of spoofing and the spoofing fault is way above the detection threshold. This allowed the estimator to reject the corresponding observation and use only the good ones. The same scenario was tested by integrating a MH grade INS with the N grade GPS, to check whether a poor quality INS sensor can still provide a desirable detection performance. Though the fault detection was successful in N-MH combination, there was a slight reduction in the test statistic value compared to the N-T combination, indicating a marginal detection. This is also due to the fact that the process noise of the sensor errors is higher in this case as compared to the T grade INS.

Considering the A-grade GPS and its combinations (subplots titled A-T, A-MH and A-ML), coupling of a good quality T-grade INS provided a slight advantage in the fault-identification performance, to overcome the marginal failure that occurred in using A-grade GPS alone. The A-T combination was able to detect the fault at t_s but the other combinations (A-MH and A-ML) failed. This does show that integrating a very good sensor does provide a marginal performance improvement in spoofing detection.

For the M-grade GPS, using any of the INS combinations does not provide any improvement in the overall fault identification performance. The performance deteriorates when the quality of the INS is poor. The ground trace of the user trajectory for the N-T combination with spoofing profile 1 is shown in Figure 4.3. When spoofing is turned ON at t_s, the GPS-only EKF and GPS/INS TC identified the fault in satellite PRN 30 range observation and it was rejected from positioning.

Hence the user trajectory in these two cases follow the reference and does not deviate with respect to the spoofing trajectory. Whereas the epoch-by-epoch LS included this spoofed observation and thereby deviating from the original reference trajectory. Since the GPS/INS LC follows the GPS LS for the GPS-only state estimation, the single faulty observation could not be identified as an outlier and deviates away from the reference.

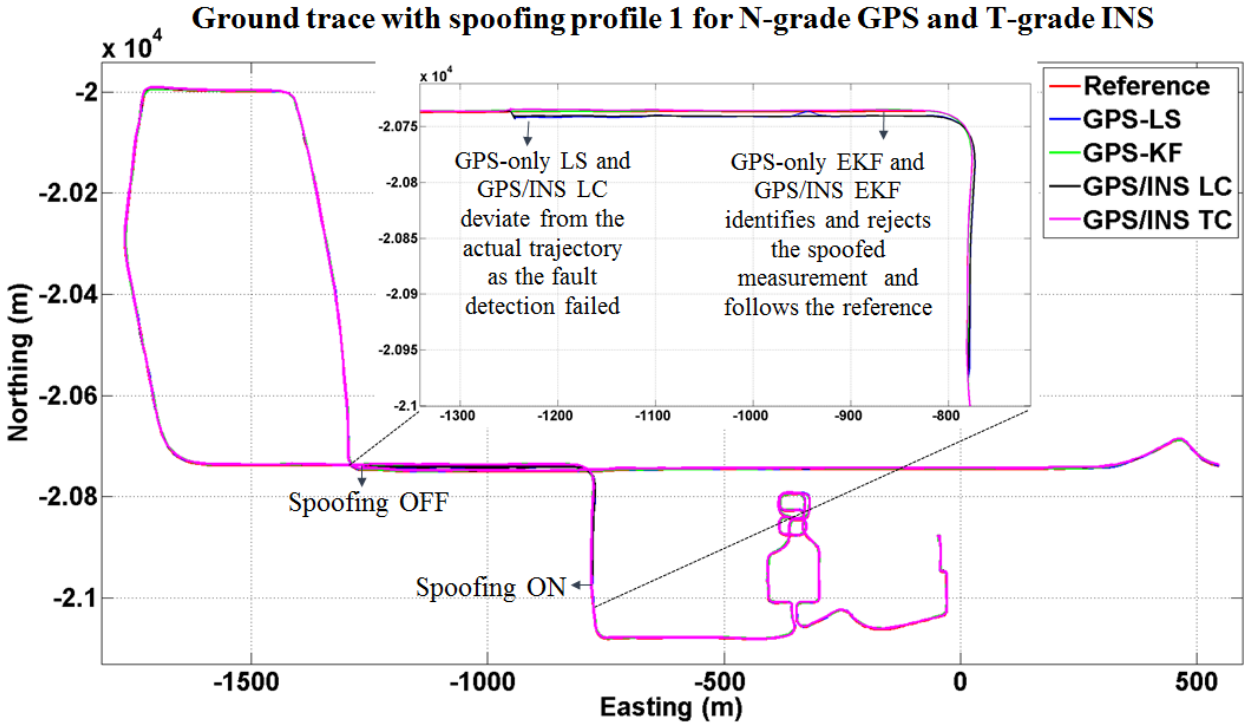

Figure 4.3: Ground Trace with spoofing profile 1 for N and N-T combination.

4.3.1.4 Fault Detection

If the measurement geometry is redundant enough, a larger magnitude of a spoofing error may be detectable. In order to observe this, magnitude of spoofing step error injected to the range observation from satellite PRN 30 is varied to test the fault detection capability of the different systems. A fault detection (global test) analysis with different magnitudes of spoofing faults is done for the GPS-only and GPS/INS TC systems. Figure 4.4 shows the plot of weighted norm of

GPS residuals/innovations at t_s plotted as a function of spoofing range error for all the GPS/INS combinations.

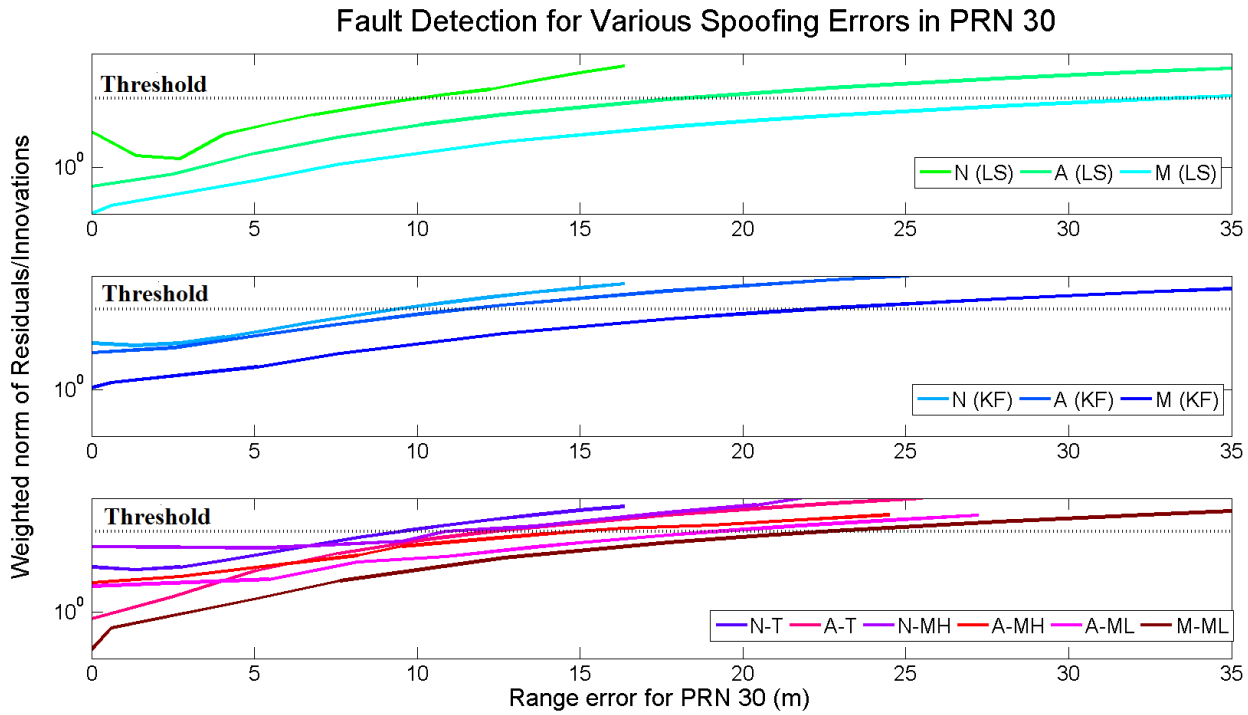

Figure 4.4: Fault detection analysis for varying spoofing errors in satellite PRN 30

Note that this is a global test analysis, where the residual/innovations of all the observations are tested together and only a single-satellite spoofing is introduced in the GPS observations. Amongst the GPS-only, all the three (N, A and M-grade) GPS receivers using EKF estimator perform better than the LS case in detecting a fault in GPS observation. In general, it can be summarized that for any given GPS receiver, using a KF based estimation provides an advantage in fault-detection performance compared to the LS case. Having INS coupled with GPS, the fault-detection performance shows a slight improvement but not significant enough to term that as an advantage. Having a poor sensor like a smartphone grade IMU does not have any improvement at all.

The A-grade and M-grade GPS receiver was able to detect the presence of an outlier at a larger magnitude of spoofing step error. Also, a spoofing range error of ~9 m or more to satellite PRN 30 would be detected in the N-grade case, but the range error induced in spoofing profile 1 at t_s is ~8 m, which is marginally lesser and therefore went undetected.

Overall, N-T combination provides the best fault detection performance amongst the other configurations. But for a vehicular automotive application, using such a high grade GPS/INS system is not economically viable. Integrating a MH or a ML grade INS with an automotive grade GPS did not provide any significant improvement in the spoofing detection performance as compared to the GPS standalone case. The quality of the GPS observations plays a critical role in determining how big of a fault can be detected. This was inferred from the covariance analysis as well.

When the fault detection was not done instantaneously, there was an increase in the overall MDB thereby making it much more difficult to detect blunders in subsequent time epochs. So the whole concept of spoofing detection works effectively only when the detector is able to detect an outlier at the first spoofing epoch t_s.

4.3.2 Spoofing Profile 2

The spoofing profile 1 provided a step change in the spoofing trajectory and the equivalent observation error, which gave a sudden change in the position at the first instant the spoofer was on. A finer way to spoof is to take the receiver out of the nominal trajectory slowly such that the GPS receiver does not recognize a sudden change. So, the second spoofing profile is chosen to provide a sudden step change in the East velocity with an error lesser than the MDB. This provides a slow ramp change in position thereby making it difficult for the filter to identify a fault in the range observation of the spoofed PRN. The position, velocity and the equivalent observation biases

for the spoofing profile 2 are shown in Figure 4.5. The local test of residuals/innovations for profile 2 is shown in Figure 4.6.

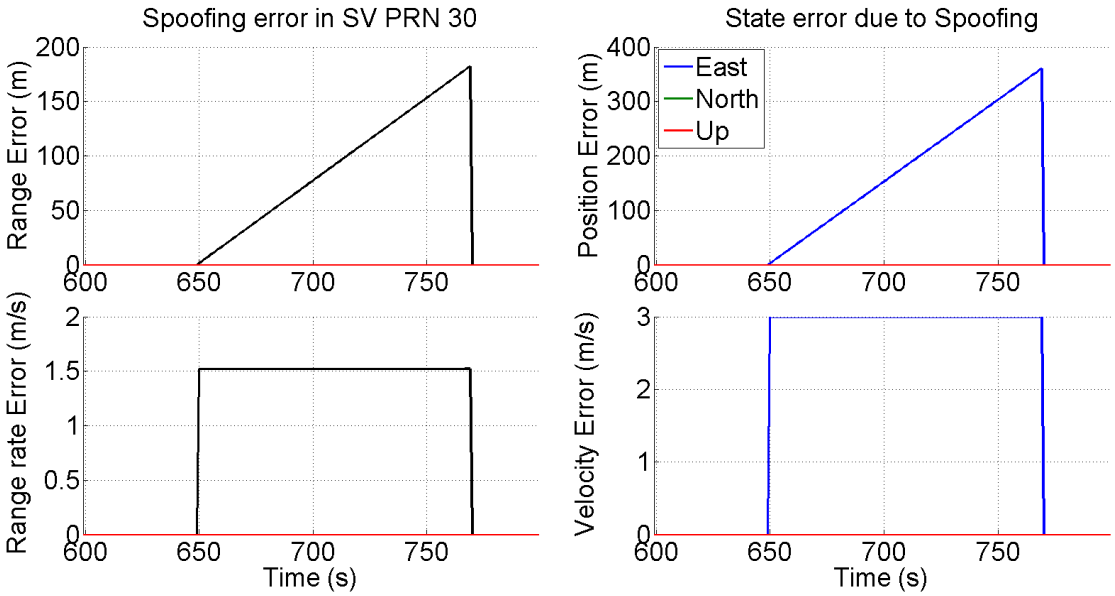

Figure 4.5: Faults due for spoofing profile 2

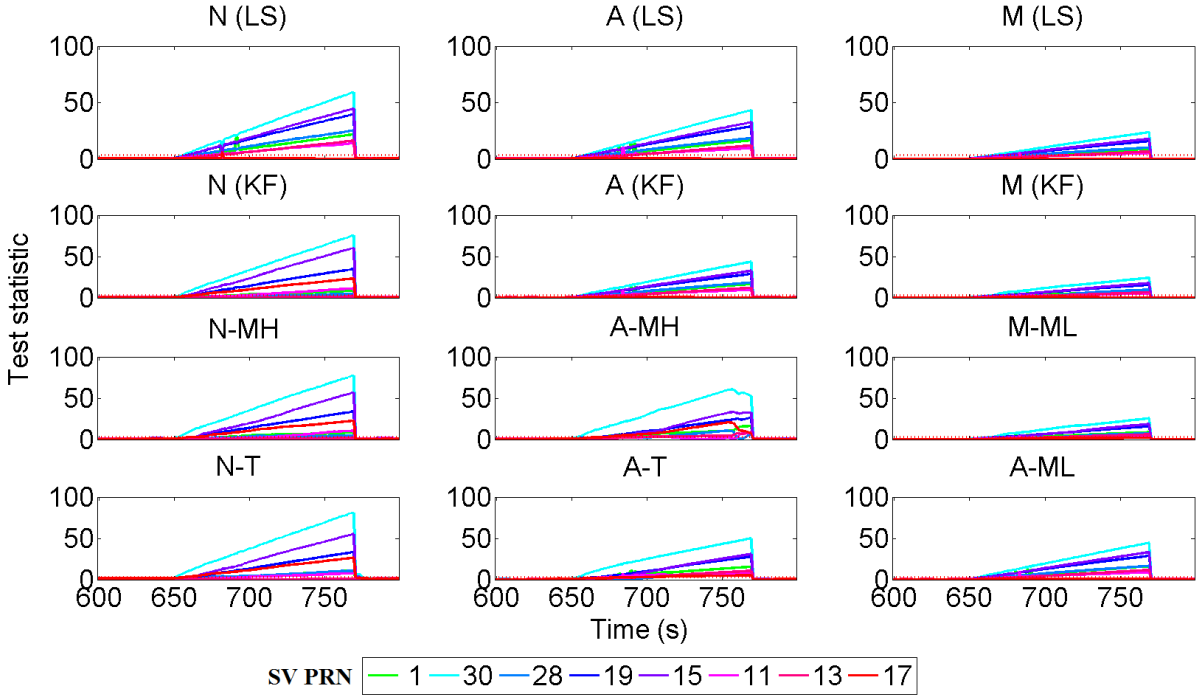

Figure 4.6: Fault identification – Spoofing profile 2

This type of spoofing attack moves the vehicle slowly away from the actual trajectory. All the estimators failed to detect the outlier in PRN 19 range observation at the first epoch because both range and range-rate faults induced due to spoofing are less than the MDB. For the EKF implementations, this allows the spoofing fault to diverge the state estimates and corrupt the other good observations over a period of time. As the magnitude of spoofing fault increases over time and once the spoofer fault exceeds the MDB, all the detectors in various combinations were able to detect the blunder. But this took approximately 20 s, during which state estimates would diverge as the faulty observations intrudes into the filter/estimator were observed.

None of the GPS and GPS/INS combinations were able to identify the fault at the first spoofing epoch. If the spoofing dynamics is increased to prove a higher velocity error, this would mean a larger step change in the range error, which will comprehend to the results obtained using spoofing profile 1 discussed in section 4.3.1.

4.3.3 Spoofing Profile 3

The third spoofing profile is much finer way of spoofing fault injection. The position, velocity and the equivalent observation faults for the spoofing profile 3 is shown in Figure 4.7 and the corresponding local test for fault identification is shown in Figure 4.8. A parabolic change in range observation is very hard to detect and can provide a very large spoofing error in short time duration. Though the spoofing duration is same as the previous profiles (120 s), the final magnitude of position error induced due to this kind of spoofing is much higher compared to previous 2 profiles and it is also much hard to detect instantaneously.

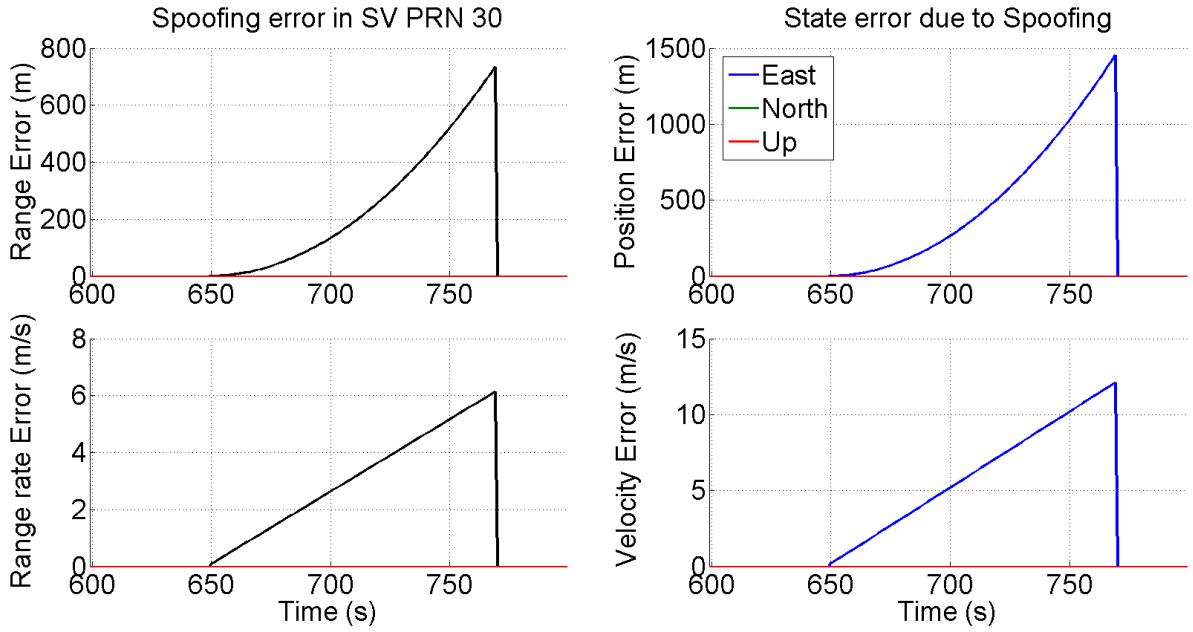

Figure 4.7: Faults due for spoofing profile 3

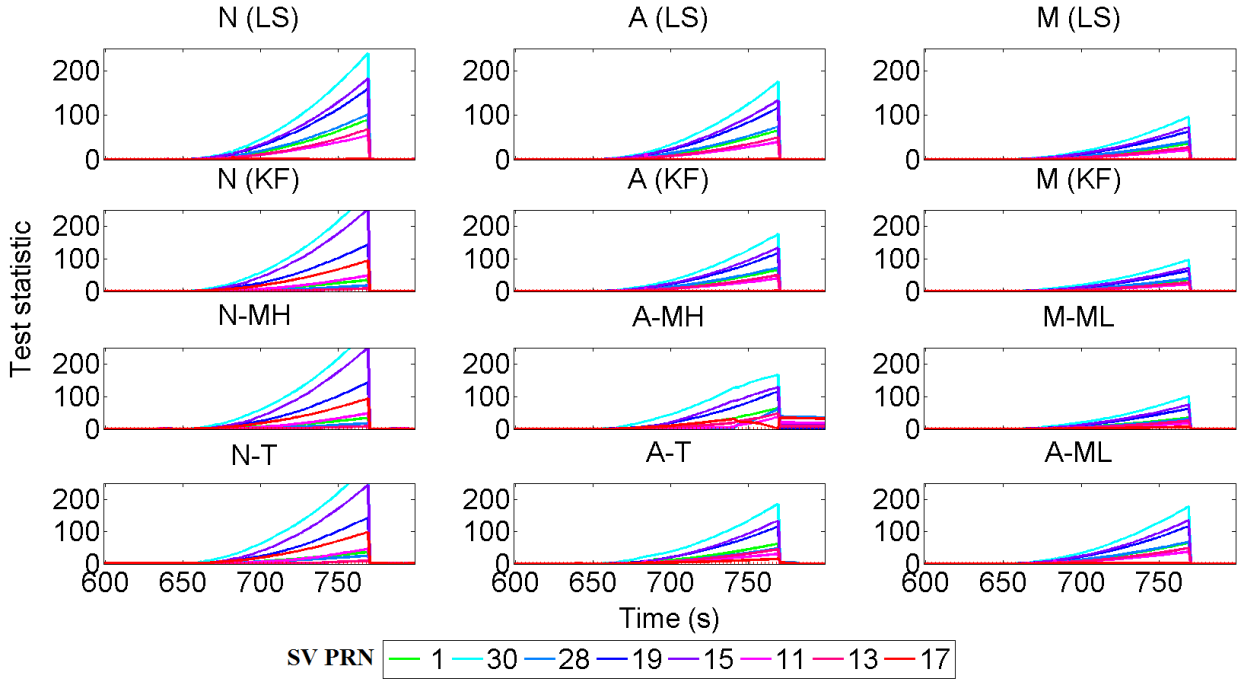

Figure 4.8: Fault identification – Spoofing profile 3

As expected, all the detectors failed to detect the fault at the very first spoofing epoch. The undetected spoofing fault corrupt the state estimates and the overall solution drifts away. Having

additional sensor observations irrespective of the sensor quality is not useful in detecting such a sophisticated spoofing attack

In the three spoofing profiles presented so far, the estimators were able to accept the good observations once the spoofing is turned off at 770 s, except for the A-MH combination in spoofing profile 3. The filter estimates started converging with the good observations immediately. This might not be the case when the spoofing duration is longer where the EKF diverges completely and reaches a point where the good measurements, when there is no spoofing, are mis-identified as faults. In order to test this, spoofing profile 4 as described in the next sub-section was tested.

4.3.4 Spoofing Profile 4

The final spoofing profile is an extension to spoofing profile 3 but with a longer duration. This was chosen to see the ability of the estimators to accept good observations after the spoofing window. The spoofing duration is increased to 180 s, which gives an east position offset of approximately 20 km at the end of spoofing window. The position, velocity and the equivalent measurement errors for the spoofing profile 4 is shown in Figure 4.9. The local test of residuals/innovations for spoofing profile 4 is shown in Figure 4.10.

In an epoch-by-epoch LS estimation, the observations at every epoch are treated independently. Therefore, when spoofing is turned off, all the good observations void of any spoofing errors are used. This can be seen at 830 s in both LS estimators plot where all the residuals lie well within the detection threshold.

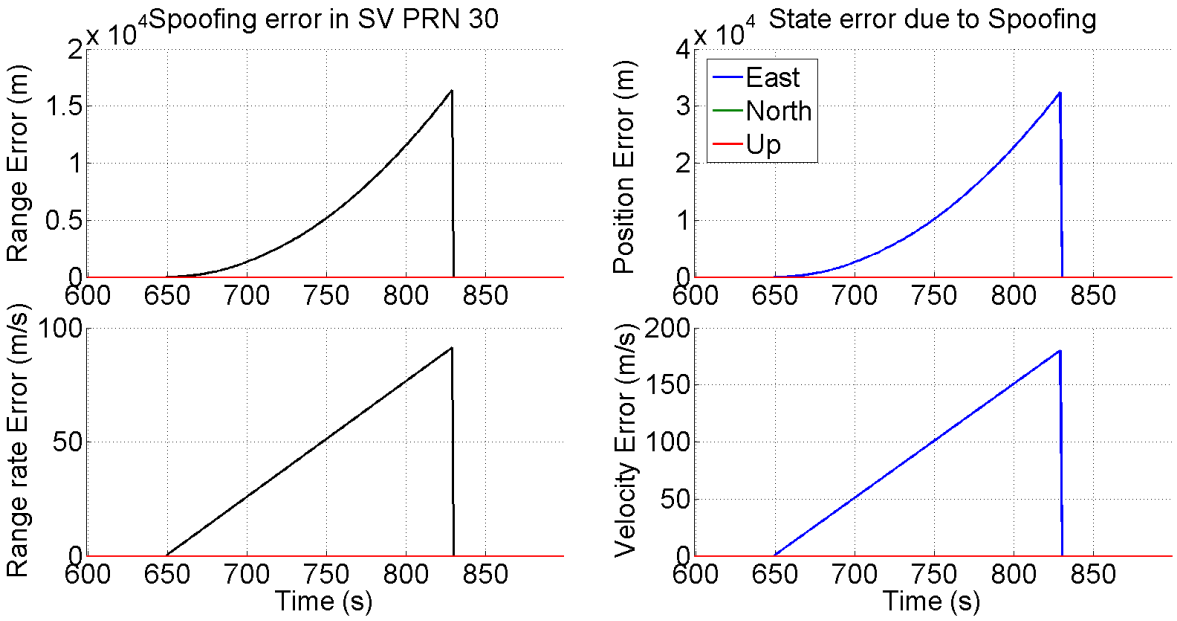

Figure 4.9: Faults due for spoofing profile 4

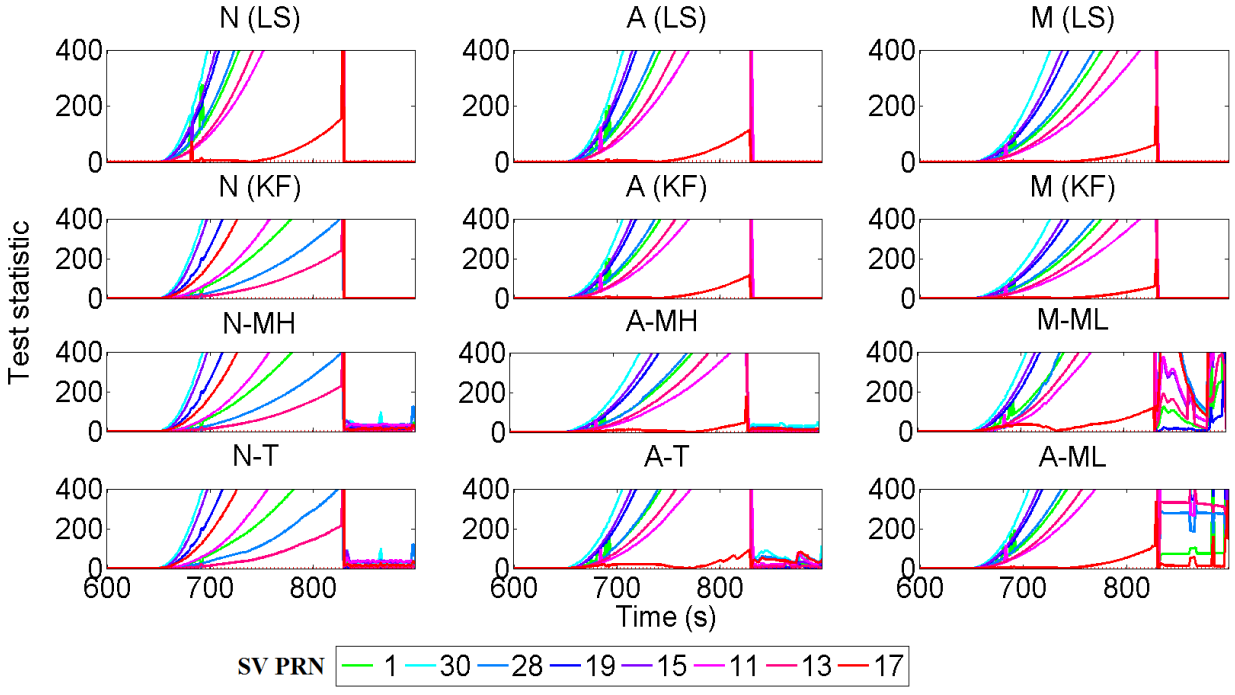

Figure 4.10: Fault identification – Spoofing profile 4

In an EKF estimator, the innovation testing of the measurements z_k depends on the predicted state estimates. If the filter state estimates and their VCM are completely diverged, then the good

observations that were available after the spoofing window will be termed as faults with respect to the deviated state estimates. This is one of the major drawback in using EKF based estimators in spoofing detection. When the quality of INS is poor, then this phenomenon occurs very quickly even for a shorter spoofing duration and this can be clearly seen in Figure 4.10. The innovations after the spoofing window are still larger than the detection threshold and the good observations are termed as faults. This would be a severe problem in using INS for spoofing detection as for longer spoofing attacks, if the spoofing is not detected at immediately at the beginning, the estimation would go wrong even after the spoofing is turned off, which does not happen in an epoch-epoch LS case.

4.4 Review of Smartphone Data Loose Coupling

The main factors that determine the GPS protection limits in using the INS for spoofing detection is the quality of the GPS and the inertial sensors used in the device. For tactical or an aerospace application, a very good quality GPS/INS is available and also affordable considering the mission requirements. But all the problems in using INS for spoofing detection is more likely in a low-cost device such as smartphones where the quality of GPS observations (also due to a relatively poor GPS antenna than the once used in high-end automotive applications) is slightly worse than the M-grade GPS module used in the tests presented in this section 4.3. Due to limitations in logging the raw GPS pseudorange and range-rate observations from the smartphone used in the above test, only the GPS position and velocity information were logged. Using this GPS and IMU data, the spoofing detection (global test) was tested in loose coupling mode.

Since individual GPS observations are not available, the spoofing simulation in this case was done by adding a position error to the GPS receiver outputs during the spoofing injection window. This is equivalent to a scenario where all the GPS observations have been spoofed and the GPS

receiver solution is completely following the spoofing trajectory. The test in LC mode was to verify the capability of the LC filter to detect this fault in the GPS receiver output at the first epoch of the spoofing attack t_s. The spoofing profile was similar to spoofing profile 1 explained in section 4.3.1.4, where a series of step spoofing error was induced to a chosen GPS observation. The difference in this test is that the various values of step spoofing faults were induced in GPS east position output from the GPS receiver during the spoofing attack window starting at t_s. Note that in case of LC, the GPS observations are the position and velocity estimates from GPS receiver and a global test on the innovations with the redundant INS position and velocity state estimates were performed. Figure 4.11 shows the global test static at t_s (first spoofing epoch) as a function of different spoofing errors in GPS east position (the black dotted line indicating the spoofing fault detection threshold).

Even an instantaneous step position error of less magnitude would go undetected in this case. From Figure 4.11 , the LC filter could only detect a fault in the GPS output when the spoofing step error exceeded 57 m at the first epoch and failed to detect any fault below this magnitude for the chosen smartphone device. A better receiver and a better GPS observation would improve the detection performance whereas a better IMU could only provide a marginal improvement as seen from the results in section 4.3. A better quality IMU could also provide better navigation performance in the absence of GPS (when GPS solution is rejected when a fault is identified). The drawback in this approach is the entire GPS solution would be rejected even if there is an fault in one or few of the GPS observations that causes the entire solution to diverge. Fault identification of individual observations are not possible in LC mode. On the positive side note, it is easier to implement LC method as it does not require any significant hardware or software change as it uses the standard outputs given by GPS/IMU sensors.

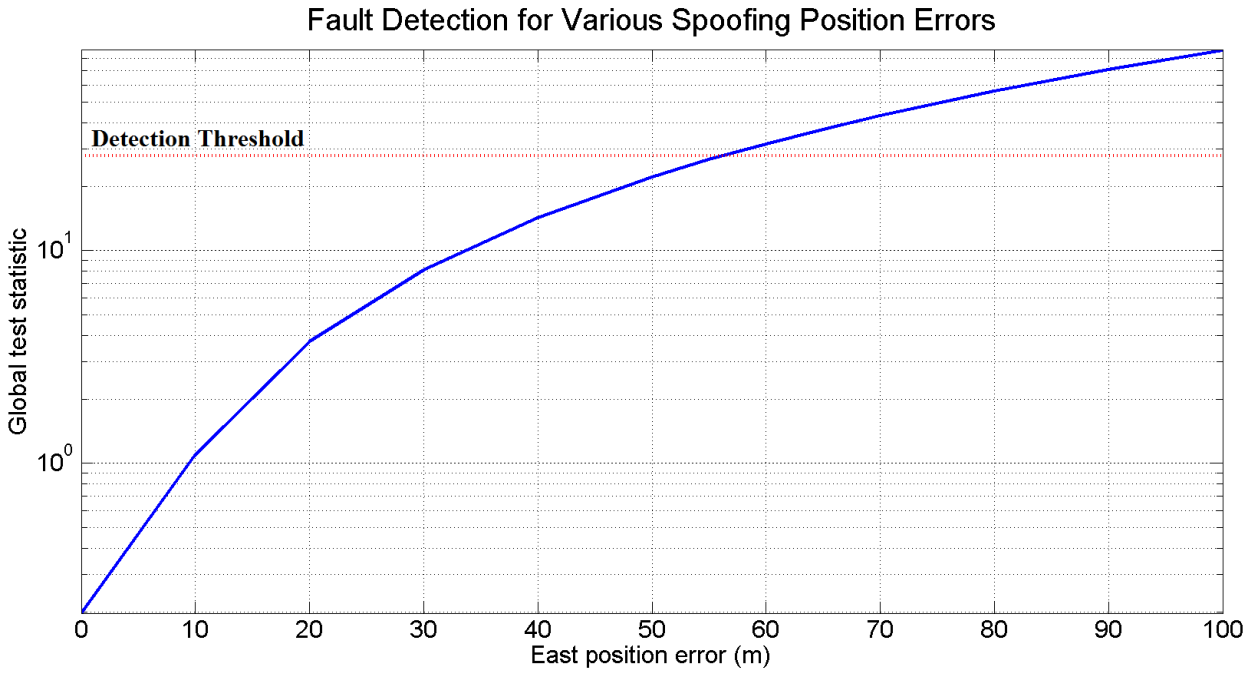

Figure 4.11: Fault detection for various spoofing error in position for smartphone data in LC mode

4.5 Summary of Results

From the simulation and actual data results, the following can be summarized:

- For a lower spoofing dynamics and longer spoofing duration, both tactical and MEMS grade sensors fail to detect the GPS spoofing fault immediately. Whereas, when the spoofing dynamics were high, the T-grade sensor perform better than the MEMS (MH and ML) grade sensors in detecting outliers in the GNSS observations, as expected. If the GNSS errors were not detected quickly, the MDB tends to increase during the spoofing window and the detection capability deteriorates further.
- A general statistical reliability analysis gives a measure of the MDB values with a chosen probability of false alarm and missed detection (α, β respectively). Though, this can be estimated theoretically for any given GPS receiver and GPS/INS combination as presented

in this thesis, if the spoofing error is not detected instantly then these theoretical estimates tend to increase over time with respect to the magnitude of the spoofing fault.

- The quality of GPS receiver plays a more significant role in spoofing detection than the INS sensor grade. A good GPS receiver integrated with a poor INS (say N-MH) performs better in spoofing detection than a bad GPS receiver integrated with a very good quality INS (say A-T).
- From the results presented in the thesis, the N-T combination provide the best performance in fault detection. But it is not desirable in terms of cost and size to accommodate such high grades of GPS/INS system in an automotive application.
- Considering the available quality of automotive GPS (A) and MEMS grade IMUs (MH), integrating the two systems does provide a slightly better spoofing detection/identification performance compared to using GPS in standalone mode with LS estimator. This can be observed from Figure 4.4, where the A-MH combination provides fault detection even at lower values of spoofing errors compared to that standalone A grade GPS in LS case. Also, having a higher grade sensor with poor GPS (say A-T) does not provide any significant improvement compared to A-MH.
- For all the GPS stand-alone and GPS/INS combinations, the fault detection works only when there is a sudden step change in the range or range-rate (Doppler) error with a magnitude higher than the MDB occurring at the first spoofing epoch. If the spoofing fault is induced slowly as shown in spoofing profiles 2, 3 and 4, the detection fails at the first epoch and the probability of providing a reliable solution during the spoofing window is reduced.

- For a typical automotive test scenario as presented in this thesis, a high-end MEMS grade (MH) sensor integration provide a very small improvement in spoofing detection performance, whereas a low-end smartphone grade MEMS sensor (ML) provide a considerably lower performance.
- The major limitation in using the low quality MEMS (ML) grade sensors are the large uncertainties in the sensors errors that are difficult to model properly. This has direct impact on the fault detection performance as shown in the MDB values as well as the actual data results presented in A-ML and M-ML combinations in Figure 4.1. If the faulty GPS observation is not detected instantly, the error does get accumulated rapidly over a short duration of time and the estimation filter drifts away from the reference trajectory. When the spoofing duration is long enough to take way the target receiver far from the reference trajectory, the filter could reject the authentic GPS observations even when the spoofer is turned OFF. This was evident in results obtained from spoofing profile 4 shown in Figure 4.10 for A-ML and M-ML combinations.
- Having a tightly-coupled GPS/INS integration for automotive applications with a high-end MEMS (MH) helps in detection and identification of individual faults in GPS observations better than the standalone GPS. Using a better INS help in better navigation performance comparted to a poor INS during the spoofing window when the faulty GPS observations are rejected, similar to a case of GPS-outage situation.
- Having a tightly-coupled integration in smartphone applications would require a significant change in the existing architecture. Considering the fact that the spoofing detection improvement achieved was not that that significant, it is not a worthwhile proposition to do a tight-coupling architecture for this purpose. But a simpler approach of loose-coupling

can be done in mobile phone applications, whose results were shown in section 4.4. The only disadvantage in case of loose coupling would be that individual GPS measurement faults could not be identified, and the entire GPS solution is discarded. Also, sophisticated finer spoofing errors on fewer observations could go undetected as the impact of those finer measurement errors on the overall navigation solution is much lower.

The results obtained from actual GPS/IMU data was analysed and presented in this chapter. Following chapter presents concluding remarks and the recommendations for future work to extend this study and analysis further.

Chapter Five: CONCLUSIONS AND RECOMMENDATIONS

In Chapter Three, the covariance analysis of the various systems was done to obtain a theoretical estimate of MDBs for all the systems under test and these were verified in Chapter Four with the experimental analysis using actual data. The major results and their significance are reviewed below, followed by recommendations for future investigation.

5.1 Conclusions

The primary motivation behind this work was to analyse the usability of the redundant INS measurements available in GPS/INS integrated systems for detecting measurement error(s) introduced due to an intentional spoofing attack on GPS observations. It is well-known that spoofing GPS observations would not affect the INS outputs and so the possibilities of using these redundant INS observations to detect/identify an error in GPS was investigated using the basic fault detection/identifications methodologies used in the chosen filter/estimators. The two most common estimators used in GPS navigation applications, which are epoch-by-epoch LS and extended Kalman Filter were chosen for the analysis and comparison.

Before proceeding with the experimental analysis using the GPS/INS integrated systems, it was necessary to understand the fault detection/identification capability of the GPS-only system assuming a single-satellite spoofing error being induced. This would provide a baseline to study whether integrating INS observations would provide any performance improvement in spoofing fault detection/identification. The GPS and INS observations were processed in the following configurations:

- GPS-only observations processed using epoch-by-epoch LS
- GPS-only observations processed using EKF
- GPS and INS integrated processing in loose-coupling mode

- GPS and INS integrated processing in tight-coupling mode

For the purpose of this study and analysis, three different grades of GPS receivers IMUs were chosen as shown in Figure 1.1, The theoretical limits of using an epoch-by epoch LS estimator and an EKF estimator in GPS-only mode were analysed using standard statically internal reliability analysis for all the three difference receiver grades. This provided an estimate of the MDB for the GPS observations for a given GPS receiver. Subsequently, the three IMU grades chosen were coupled (loose and tight mode) with the GPS receivers to form six GPS/INS combinations as shown in Figure 1.1 and the covariance analysis was repeated for each of those combinations. A sub-urban land vehicular motion trajectory was chosen, which could be a representation of typical automotive application. Following were the inferences made from the covariance analysis results:

- The MDB is mainly a function of the GPS receiver measurement accuracy even in case of GPS/INS integrated systems. The IMU measurement quality play a very minor role in the overall MDB performance of GPS observations.
- The magnitude of MDB (related to the fault detection/identifications) depends on the number of available good observations and the satellite geometry. In a dynamic user environment where the observation geometry changes or in regions of high blockage and foliage where the number of observations are less and noisy, the MDB values are high thus making it difficult to detect spoofing attacks with finer trajectory changes.
- EKF estimator provides better fault-detection performance for single-satellite spoofing errors compared to that of an epoch-by-epoch LS estimation. This is due to the fact that the time evolution of the state vectors was taken into account in an EKF estimator, where a variation of MDB with respect to the changes in the observation geometry is much

smoother and relatively lower MDB values in epochs of less number of observations were observed as compared to the epoch-by-epoch LS case (), provided the system dynamics and uncertainties are modelled properly.

- Coupling of INS with GPS provides a marginal improvement in the detection/identification performance of faulty GPS observations, whereas coupling a poor quality IMUs (ML) as the ones used in smartphones with an automotive grade GPS receiver (A) significantly increases the MDB values in epochs where the number of observations are less (indicated by a higher value of MDB) compared to A-grade receiver coupled with a MH-grade IMU. This is mainly due to the fact that there exists a high-level of sensor error model uncertainties as the modelling those for such a poor quality IMU is very difficult.

The covariance analysis presented in this thesis is a useful tool for navigation system designers to investigate the requirement of the GPS/INS sensor grade for spoofing detection considering the size, cost and safety requirements of an automotive consumer grade application.

In order to test the theoretical results obtained from the statistical reliability analysis, actual authentic GPS and IMU data was collected in the same sub-urban vehicular trajectory used. The data was processed using the software implemented in MATLAB™ in the four configurations mentioned in section Chapter Five:. A configurable spoofing generator module was added in order to add observations errors to the chosen satellite(s) with respect to a spoofing trajectory. The use of inertial sensors in detecting and identifying the fault in spoofed GPS observation was investigated for different grades of GPS/INS integrated systems. Following were inferences made from the results from actual data:

- As inferred in the statistical reliability analysis. it was shown that GPS receiver quality requirement is the primary factor for the spoofing detection.

- Both MEMS and Tactical grade sensors performance was undesirable in a worst case spoofing profile when the spoofing dynamics is less and for longer duration. The challenges and limitations in using MEMS grade sensors were investigated. Based on the results obtained, the effectiveness in using tight coupling architecture in an automotive and mobile phone application to detect GNSS errors was discussed.
- The challenges and limitations in using MEMS grade sensors for spoofing detection were investigated. Results show that using a MEMS grade sensor in a coupled system (loose or tight) does not provide significant improvement. Also, the spoofing error if not detected instantly the error accurately far more rapidly than the higher grade sensors.
- Based on the results obtained, the effectiveness in using tight coupling architecture to detect GNSS errors was presented. Considering the marginal improvement provided by the INS integration and then only in case of a good quality INS, it is not a worthwhile proposition to have a tight-coupling architecture in smartphones for enhancing the spoofing detection capability.
- The loose coupling of GPS/INS in smartphones is effective in detecting larger magnitude spoofing errors. Future enhancements in inertial sensor quality in smartphones would provide better signal authentication performance.

The results presented in the thesis provides an understanding of the spoofing detection capability for consumer grade automotive GPS manufacturers. For example, in a typical road tolling and freight tracking application to detect the intentional manipulation of the navigation information.

To conclude, this thesis presented a comparative study and analysis of GNSS fault detection/identification limits that can be achieved from the different GNSS/INS combinations specified for an automotive application.

5.2 Recommendations for future work

Based on the work and results obtained from this work, following are the recommendations for the future work:

- This work focussed only on the comparative study of GPS spoofing detection using various grades of INS in a single frequency GPS L1 receiver. A logical extension of the same study shall be done for a multi-frequency GPS receiver to investigate the impact of the second frequency signal in the overall spoofing detection performance.
- With additional GNSS constellations such as GLONASS being fully operational, the GNSS spoofing detection performance in a multi-constellation receiver scenario can be analysed.
- Multi-satellite spoofing scenarios can be tested to further investigate the performance for GPS-only and various grades of GPS/INS combinations. This also helps in understanding the multiple blunder detection performance of the estimators used in different GPS/INS combinations.
- Carrier phase observations were not considered in this work. The impact of using this can be analysed in future work to see whether it provides any improvement in the overall fault detection/identification performance.

References

Akos, D. M. (2012). "Who's Afraid of the Spoofer? GPS / GNSS Spoofing Detection via Automatic Gain Control (AGC)". in *NAVIGATION, Journal of the Institute of Navigation*, Vol. 59, pp. 281–290.

Baarda, W. (1967) "Statistical concepts in geodesy," *Netherlands Geodetic Commission*, 4(2), Delft, Netherlands.

Baarda, W. (1968) "A Testing Procedure For Use In Geodetic Networks," in *Publications on Geodesy Netherlands Geodetic Commission*, 5(2), Delft, Netherlands.

Borio, D., L. Camoriano, & L. Lo Presti, (2008) "Two-Pole and Multi-Pole Notch Filters : A Computationally Effective Solution for GNSS Interference Detection and Mitigation", in *IEEE Systems Journal*, vol.2, no. 1, March 2008, pp. 38–47.

Brown, R. G., & P.Y.C. Hwang (1997) *Introduction to Random Signals and Applied Kalaman Filtering*. John Wiley and Sons.

Caparra, G., C. Wullems, S. Ceccato, S. Sturaro, N. Laurenti, O. Pozzobon, R.T.Ioannides, M. Ceisci, (2016) "Design Drivers and New Trends for Navigation Message Authentication Schemes for GNSS Systems". *InsideGNSS*, September/October 2016, pp. 64–73.

Correia, M. J., (2013) *Towards an Anti-spoofing System Based on Phase and Modulation Features*, Technical Report RT/28/2013, Instituti de Engenharia de Sistemas e Computadores Investigcaso e Desenvolvimento em Lisboa, Portugal, 11 pages.

Department of Defense (2013) *Navstar GPS Space Segment/Navigation User Interfaces (ICD-GPS-200H)*.

Gelb, A. (1974). *Applied Optimal Estimation*. The M.I.T Press.

Godha, S. (2006*) Performance Evaluation of Low Cost MEMS-Based IMU Integrated With GPS for Land Vehicle Navigation Application*, PhD thesis, Department of Geomatics Engineering, University of Calgary, Canada.

Gromov, K. G. (2002) *Gidl: generalized interference detection and localization system*, PhD Thesis, Department of Aeronautics and Astronautics, Stanford University, U.S..

Heinrichs, G., E. Loehnert, & E. Wittmann, (2010) "User RAIM Integrity and Interference Mitigation Test Results with Upgraded German Galileo Test Range GATE", in *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, NAVITEC 2010*, Noordwijk, 7 pages.

Heng, L., D.B. Work, & G.X. Gao (2013) "Cooperative GNSS Authentication", *InsideGNSS*, September/October 2013, pp. 70–75.

Hopfield, H. S. (1971) "Tropospheric effect on electromagnetically measured range: Prediction from surface weather data", in *Journal of Radio Science*, vol. 6, no. 3, March 1971, pp. 357–367.

Humphreys, T. E. (2013) "Detection strategy for cryptographic gnss anti-spoofing", in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090.

Humphreys, T. E., B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, & P.M Kintner, (2008) "Assessing the spoofing threat: Development of a portable GPS civilian spoofer", in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation*, 16-19 September, Savannah, GA, pp. 2314–2325.

Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen, & G. Lachapelle, (2012). GPS spoofer countermeasure effectiveness based on signal strength , noise power , and C/ N0 measurements, in *International Journal of Satellite Communications and Networking*, vol. 30, pp. 181–191. http://doi.org/10.1002/sat

Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen, & G. Lachapelle, (2012) "GPS vulnerability to spoofing threats and a review of antispoofing technique", in *International Journal of Navigation and Observation*, Vol. 9, Article ID 127072, 16 pages

Jafarnia-Jahromi, A., S. Daneshmand, & G. Lachapelle, (2013) "Spoofing Countermeasures for GNSS Receivers – A Review of Current and Future Research Trends", in *4th Intern Colloquium on Scientific and Fundamental Aspects of the Galileo Programme*, 4-6 December 2013, Prague, pp. 4–6.

Jahromi-Jahromi, A. J. (2013) *GNSS Signal Authenticity Verification in the Presence of Structural Interference*, PhD thesis, Department of Geomatics Engineering, University of Calgary, Canada.

Jakeli. C. (2001). *Inertial Navigation Systems with Geodetic Applictions*. Berlin; New York: de Gruyter.

Kalman R.E. (1960) "A New Approach to Linear Filtering and Prediction Problems", in *Transactions of the ASME– Journal of Basic Engineering*, 82 (Series D), pp. 35-45.

Kaplan, E. D., & C. J. Hegarty (2006). *Understanding GPS: Principles and Applications, Second Edition*, Artech House.

Kay, S. M. (1993). *Fundamentals of Statistical Signal Processing - Estimation Theory*. Prentice Hall Signal Processing Series.

Khanafseh, S., N. Roshan, S. Langel, Chan, Fang-Cheng Chan, M. Joerger, and B. Pervan (2014), "GPS Spoofing Detection using RAIM with INS Coupling," *Position, Location and Navigation Symposium - PLANS 2014*, Monterey, CA, USA, pp. 1232–1239.

Klobuchar, J. A. (1987) "Ionospheric Time-Delay Algorithm for Single-Frequency GPS Users", *IEEE Transactions on Aerospace and Electronic Systems*, Vol. AES-23, No. 3, pp. 323–331.

Koch, K.R. (1988). *Parameter Estimation and Hypothesis Testing in Linear Models*, Springer-Verlag New York, Inc. NY, U.S., ISBN:0-387-18840-1

Kuhn, M. G. (2010). *Signal Authentication in Trusted Satellite Navigation Receivers*, Springer Berlin Heidelberg, pp. 331-348.

Kuhn, M. G. (2004). *An Asymmetric Security Mechanism for Navigation Signals*. International Workshop on Information Hiding, Springer-Verlag Berlin Heidelberg, pp. 239–252.

Lachapelle, G., & M.E. Cannon (2014) *Lecture Notes for ENGO 625 - Advanced GNSS Theory and Applications.*

Ledvina, B., W.J. Bencze, B. Galusha, & I. Miller, (2010) "An In-line Anti-Spoofing Device for Legacy Civil GPS Receivers", in *Proceedings of the 2010 International Technical Meeting of The Institute of Navigation*, 25-27 January, San Diego, CA, U.S., pp. 698-712

Lindström, J., D.M. Akos, O. Isoz, & M. Junered (2007) "GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules", in *Proceedings of the ION GNSS 2007*, 25-28 September, Fort Worth, TX, U. S., pp. 1165-1172.

Misra, P., & Per Enge (2001) *Global Positioning System - Signals, Measurements, and Performance*. Ganga-Jamuna Press.

Montgomery, P., T.E. Humphreys, B.M. Ledvina (2009) "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer", in *Proceedings of ION ITM 2009*, 26-28 January, Anaheim, CA, U.S., pp. 124–130.

Montgomery, P. Y., T.E. Humphreys, & B.M. Ledvina (2009) "A Multi-Antenna Defense Receiver-Autonomous GPS Spoofing Detection", *InsideGNSS*, March/April 2009, pp. 42–46. Multi-Antenna Defense.

Department of Defense (2013). *Navstar GPS Space Segment/Navigation User Interfaces (*IS-GPS-800).

Noureldin, A., T. B. Karamat, J. Georgy (2014). *Fundamentals of Inertial navigation, Satellite-based Positioning and their Integration*. ISBN 978-3-642-30466-8 (eBook), Springer, New York

Parkinson, B.W., J.J. Spilker Jr, P. Axelrad, Per Enge (1996) *Global Positioning System, Volume 2 - Theory and Applications*, American Institute of Aeronautics and Astronautics, Washington, DC.

Petovello, M. G. (2003) *Real-Time Integration of a Tactical-Grade IMU and GPS for High-Accuracy Positioning and Navigation*, PhD thesis, Department of Geomatics Engineering, University of Calgary, Canada.

Petovello, M. G. (2013) *Lecture Notes for ENGO 620 - Estimation for navigation*, ENGO 620 Course Notes, Department of Geomatics Engineering, University of Calgary, Canada.

Pozzobon, O., L. Canzian, M. Danieletto, & A.D. Chiara (2010) "Anti-spoofing and open GNSS signal authentication with signal authentication sequences", in *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, NAVITEC 2010*, Noordwijk, pp. 1-6.

Psiaki, M. L., Hanlon, B. W. O., Bhatti, J. A., Shepard, D. P., & Humphreys, T. E. (2013) "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals", *IEEE Transactions on Aerospace and Electronic Systems, Vol. 49*, No.4, pp. 2250–2267.

Ray, J. K. (2000) *Mitigation of GPS Code and Carrier Phase Multipath Effects Using a Multi-Antenna System*, PhD thesis, Department of Geomatics Engineering, University of Calgary, Canada, pp.27-35

Ryan, S. J. (2002) *Augmentation of DGPS for Marine Navigation*, PhD thesis, Department of Geomatics Engineering, University of Calgary, Canada, pp.12-85.

Scott, L. (2003) "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems", in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, 9-12 September, Portland, OR, U. S., pp. 1543–1552.

Scott, L. (2012) "Spoofs, Proofs & Jamming - Towards a Sound National Policy for Civil Location and Time Assurance", *InsideGNSS*, September/October 2012, pp. 42–53. (Available at http://www.insidegnss.com/node/3183)

Seco-Granados, G., J.A. Fernandez-Rubio & C. Fernandez-Prades (2005) "ML estimator and hybrid beamformer for multipath and interference mitigation in GNSS receivers". *IEEE Transactions on Signal Processing*, Vol. 53, No.3, March 2005, pp. 1194–1208.

Skone, S. (1998). *Wide Area Ionospphere Grid Modelling in Auroral Region*, PhD thesis, Department of Geomatics Engineering, University of Calgary, Canada, pp.7-27

Steeves C., R. Fraser (1987) "Statistical Post-Analysis of Least Squares Adjustment Results", in *Papers For the CISM Adjustement and Analysis Seminars , Krakiwsky, Edward, ed. Canadian Institute of Geomatics*, (pp. 182–210).

Tanil, C., S. Khanafseh, and B. Pervan (2015) "GNSS Spoofing Attack Detection using Aircraft Autopilot Response to Deceptive Trajectory GNSS Spoofing Attack Detection using Aircraft Autopilot Response to Deceptive Trajectory", in *Proceedings of ION GNSS+ 2015*. 14-18 September, Tampa, FL, U.S., pp. 3345-3357

Wen, H., P. Huang, J. Dyer, A. Archinal, & J. Fagan (2005) "Countermeasures for GPS signal spoofing", in *Proceedings of ION GNSS 2005*, 13-16 September, Long Beach, CA, U. S., pp. 1285-1290.

Wesson, K. D., M.P. Rothlisberger, & T.E. Humphreys (2011) "A Proposed Navigation Message

Authentication Implementation for Civil GPS Anti-Spoofing", in *Proceedings of the ION GNSS 2011*, 21-23 September, Portland, OR, U. S., pp. 3129 - 3140

Wesson, K. D., D. P. Shepard, J. A. Bhatti, & T.E. Humphreys (2011) "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-spoofing", in *Proceedings of the ION GNSS 2011*, 20-23 September, Portland, OR, U. S., pp. 2646 - 2656

Wesson, K., D. Shepard, and T. Humphreys (2012) "Straight talk on anti-spoofing: Securing the future of PNT," *GPS World*, January 2012, pp. 32-63.

Wieser, A., M.G. Petovello, G. Lachapelle, (2004) "Failure Scenarios to be Considered with Kinematic High Precision Relative GNSS Positioning", in *Proceedings of the ION GNSS 2004*, 21-24 September, Long Beach, CA, U. S., pp. 1448-1459.

Wittmann, E., T. Zink, G. Heinrichs, D. Lekaim, D., Delfour, D. Joly, M. Jeannot, M. Tossaint (2012) "The GATE Test Infrastructure and its Use for Galileo Integrity Tests to Support ESA` s European GNSS Evolution Programme", in *Proceedings of the ION GNSS 2012*, 17-21 September, Nashville, TN, U. S., pp. 2818-2827

Zhang, J. (1999). *Investigations into the Estimation of Residual Tropospheric Delays in a GPS Network*, PhD thesis, Department of Geomatics Engineering, University of Calgary, Canada.